

Entry-Exit-System

Das EES soll Grenzübertritte von Nicht-EU Bürgern über viele Jahre speichern. Es ist sozusagen das Gegenstück zu [[VIS]] für visafreie Länder (die VIS-Opfer sollen aber zusätzlich auch im EES erfasst werden, etwa um „overstayer“ einheitlich zu erfassen.. Es war schon im Stockholm-Programm von 2010 vorgesehen, galt aber lange Jahre als zu durchgedrehte Vorratsdatenspeicherung.

Seit 2017 wird das System jetzt bei [[EU-LISA]] aufgebaut.

[[<https://www.statewatch.org/news/2022/november/schengen-border-crossing-times-to-increase-massively-when-new-database-comes-into-use/>|Statewatch berichtet 11/2022]], dass das System im Mai 2023 wirklich laufen soll.

Operativer Teil des Plans ist eine Plattform zur Anmeldung, das ETIAS.

Dieser Zeitplan wird zwar im

[[https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Taetigkeitsberichte/31TB_22.html|31. TB des LfDI für 2022]] (S. 54) bekräftigt, aber am Schluss ist es doch anders gekommen:

[[<https://netzpolitik.org/2023/superdatenbank-ees-zum-vierten-mal-verschoben-eu-direktorin-stellt-keine-schadenersatzforderungen-an-frueheren-arbeitgeber/>|Netzpolitik.org berichtet im Juni 2023]], dass Reisende wohl bis Sommer 2024 verschont bleiben (und noch von erwartbaren Filzlagen rund ums EES).

= Rechtsgrundlagen =

EES und ETIAS sind geregelt in <<Ratsdokument(EU 2017/2226)>> (im Folgenden EESVO) und <<Ratsdokument(EU 2018/1240)>>. In der BRD sollen zwei Umsetzungsgesetze hinzukommen, das EES-Durchführungsgesetz EESDG und das ETIAS-Durchführungsgesetz ETIASDG. Diese sind seit Dezember 2022 im parlamentarischen Verfahren; siehe <<BtDS(20/5333)>>.

Interessanterweise ruft Art. 39 EESVO die DSGVO als Rechtsgrundlage auf und nicht, wie mensch angesichts von „Sicherheit“ und Staatsraison in der Zweckbestimmung vielleicht erwarten könnte, die JI-Richtlinie.

== Zweck der Datenspeicherung ==

Zentrales Argument der Befürworter war das Phantasma der „overstayer“, also Personen, die etwa mit Touristen- oder Studi-Visa oder für derartige Zwecke visafrei einreisen und dann nicht zur vorgesehenen Zeit wieder aureisen. Außerdem sollen leichter Einreiseverweigerungen ausgesprochen und durchgesetzt werden können. Dazu kommt hier gleich, was bei [[EURODAC]] noch fast zehn Jahre gedauert hat, nämlich der Einsatz durch Polizei und Geheimdienste. In den Worten von Erwägungsgrund 15 der EESVO

{ { { #!blockquote Ziele des EES sollten sein, das Außengrenzenmanagement zu verbessern, irreguläre Einwanderung zu verhindern und die Steuerung der Migrationsströme zu erleichtern. Das EES sollte gegebenenfalls insbesondere zur Identifizierung von Personen beitragen, die die Voraussetzungen hinsichtlich der Dauer des zulässigen Aufenthalts im Hoheitsgebiet der Mitgliedstaaten nicht oder nicht mehr erfüllen. Darüber hinaus sollte das EES zur Verhütung, Aufdeckung und Untersuchung terroristischer oder sonstiger schwerer Straftaten beitragen. } } }

Auch wer an die Migrationskontrolle glaubt, sollte zumindest beim Nachsatz höchst skeptisch werden. Artikel 6 EESVO hat das ausbuchstabiert, wobei die Migrationskontrolle in Absatz 1 steht, die nach innen gewandte Repression in Absatz 2. Absatz 3 soll die Daten den wahnsinnigen Vielreisendenprogrammen für unbesorgte Businessmen zugänglich machen (was jetzt wirklich auch per DSGVO-Einwilligung möglich gewesen wäre, wenn schon nicht (1) Lit e (Automatisierung von Grenzkontrollen) als einschlägig gesehen wird).

Im Bereich der Strafverfolgung postuliert die EESVO eine Art Subsidiarität, nach der EES-Daten erst dann abgefragt werden sollen, wenn andere, vor allem nationale, Systeme nicht weitergeführt haben. Dass das so nicht rauskommen wird, macht z.B. die im [\[\[https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Taetigkeitsberichte/30TB_21.pdf?__blob=publicationFile&v=13|30. TB des BfDI für 2020\]\]](https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Taetigkeitsberichte/30TB_21.pdf?__blob=publicationFile&v=13|30) berichtete Erfahrung mit [\[\[VIS\]\]](#)-Abfragen durch die FIU (cf. [\[\[Datenbanken des Zoll\]\]](#)) klar:

{ { { #!blockquote Es wurden VIS-Recherchen durchgeführt, obwohl die sie betreffenden Personen kein Schengen-Visum benötigten. Dabei wurde nicht hinreichend geprüft und dokumentiert, weshalb davon ausgegangen wurde, dass die Vorgaben des VIS-Zugangsbeschlusses vorlagen. } } }

Im Klartext: Die FIU-Leute haben einfach blind und immer alles „mit Ausländern“ ins VIS gehauen, und dass das eigentlich verboten ist, ist bis zur Kontrolle des BfDI niemandem aufgefallen.

== Gespeicherte Daten ==

Gespeichert werden sollen im Wesentlichen alle Grenzübertritte von Menschen, die nicht Schengen-Bürger sind und nicht ohnehin schon in [\[\[VIS\]\]](#) erfasst sind; Art. 2 der EESVO definiert die Speicheropfer in schmerzhaftem Detail. Insbesondere werden auch verweigerter Grenzübertritte gespeichert, also Zurückweisungen an der Grenze (mit Ausnahme illegaler Pushbacks, natürlich).

Nach Art 16 sind die Stammdaten der Speicheropfer:

- Nachname (Familiename), Vorname oder Vornamen, Geburtsdatum, Staatsangehörigkeit oder Staatsangehörigkeiten,
- Art und Nummer des Reisedokuments oder der Reisedokumente sowie dem aus drei Buchstaben bestehenden Code des ausstellenden Staates;
- dem Datum des Ablaufs der Gültigkeitsdauer des Reisedokuments oder der Reisedokumente;
- ein biometrisches Gesichtsfoto
- biometrische Fingerabdrücke einer Hand (ggf. aus [\[\[VIS\]\]](#) importiert, wenn das Speicheropfer visumpflichtig ist)

- ein Overstayer-Flag, das gesetzt wird, wenn am Ende der berechneten Aufenthaltsdauer keine Ausreise gespeichert wurde.
- allerlei Status-Info, welche Behörden jeweils gerade welche Entscheidungen zum Aufenthaltsstatus der Opfer getroffen haben.

Dazu kommt bei jedem Grenzübertritt:

- Datum/Uhrzeit des Grenzübertritts
- Grenzübergangsstelle
- Details zur Art eventueller Kurzzeitvisa

Ein bitterer Scherz ist dabei Art. 17 (5):

{{{#!blockquote Die Mitgliedstaaten gewährleisten angemessene Verfahren, die die Würde der Person wahren, falls bei der Abnahme der Fingerabdrücke Schwierigkeiten auftreten. }}}}

Noch zur Biometrie: Art 15 (2) erlaubt, die Gesichtsbilder aus dem Pass auszulesen und zu speichern – ein schönes Beispiel für die schleichende Aushebelung von Datenschutzgarantien. Bei der Einführung der biometrischen Bilder hieß es ja noch, diese würden nur zur Bestätigung der Identität genutzt. Immerhin verrät Art. 15 (3), dass die Leute, die das geschrieben haben, noch ein schlechtes Gewissen hatte.

== Fristen ==

Mensch könnte meinen, der Speicherzweck sei erfüllt, wenn die Leute wieder ausgereist sind, und mithin müsste dann gelöscht werden. Das sah allerdings die Autorilla in Kommission, Rat und Parlament anders. Art. 3 sieht vor, dass die Stammdaten bis drei Jahre nach der letzten Einreise gespeichert bleiben, es sei denn, es gibt keinen Ausreisedatensatz; dann sind es fünf Jahre.

Dass das ein fieser Eingriff in die Menschenrechte ist, war auch der Autorilla klar (weshalb sie die Frist für Familienangehörige von Schengenianer_innen auch auf ein Jahr reduzieren). Sie haben dazu in Erwägungsgrund 32 folgenden Bullshit produziert:

{{{#!blockquote Mit dieser dreijährigen Datenspeicherfrist wird die Notwendigkeit häufiger Neuerfassungen reduziert, was allen Reisenden zugutekommen wird, da sich sowohl die durchschnittlich für den Grenzübertritt benötigte Zeit als auch die Wartezeit an Grenzübergangsstellen verkürzt wird. Auch für Reisende, die nur einmal in das Hoheitsgebiet der Mitgliedstaaten einreisen, verringert sich die Wartezeit an Grenzübergangsstellen, da andere bereits im EES erfasste Reisende sich vor Ablauf der dreijährigen Datenspeicherfrist nicht erneut erfassen lassen müssen. Die dreijährige Datenspeicherfrist ist ebenfalls notwendig, damit der Grenzübertritt durch automatisierte Verfahren und durch Self-Service-Systeme erleichtert und beschleunigt werden kann. }}}}

Mensch könnte angesichts dieser Bequemlichkeitsargumentation erwarten, dass Speicheropfer auf die Bequemlichkeit verzichten und vorzeitig löschen lassen können. Vermutlich ist niemand überrascht, dass Art. 35 das nicht vorsieht – nur Behörden dürfen vorzeitig löschen, wenn es für die Herrschaft angemessen erscheint.

== Übertragungen ==

An sich sollen die EES-Daten nach Art. 40f allenfalls mal kurz in nationalen Systemen gespeichert werden. In Wirklichkeit verrät ein rascher Blick auf Art. 41 EESVO, dass allerlei Übertragungen an Drittstaaten geplant sind: Art. (1) und (5) sagen kurz, dass sie nicht stattfinden sollen, die restlichen umfangreichen Absätze heben dieses Verbot dann wirksam aus.

Tatsächlich zeigt die Erfahrung mit dem VIS

(https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Taetigkeitsberichte/30TB_21.pdf?__blob=publicationFile&v=13 [30. TB des BfDI für 2020]), S. 87), dass noch nicht mal die milden Einschränkungen beachtet werden:

{ { { #!blockquote Des Weiteren wurden VIS-Daten an Drittstaaten übermittelt, ohne dass die Voraussetzungen des VIS-Zugangsbeschlusses erfüllt waren. Zudem wurden nicht alle nationalen Übermittlungsvoraussetzungen geprüft, festgestellt und dokumentiert. } } }

== Teilnehmende Behörden ==

Zugang zu den Daten – immer auch Biometrie umfassend – haben (Art. 23ff EESVO)

- Grenzbehörden (die nach persönlichen Daten, Passnummern u.dgl. suchen können und, wenn das zu nichts führt, wird nach Fingerabdrücken und Gesichtsbildern gesucht)
- Visumbehörden (also z.B. Botschaften)
- Einwanderungsbehörden
- „Benannte Behörden“ in Sachen „Verhütung, Aufdeckung und Untersuchung terroristischer oder sonstiger schwerer Straftaten abzufragen.“ In der BRD wird das wohl so aussehen, dass das [\[Datenbanken Bundesverwaltungsamt|BVA\]](#) Abfragen für Polizeien und Geheimdienste macht. Details kommen dann wohl in der EESDG.
- [\[Europol\]](#). Natürlich. oh Grusel.

Bemerkenswert Art. 31 (2):

{ { { #!blockquote In dringenden Fällen, in denen eine unmittelbar bevorstehende Lebensgefahr, die im Zusammenhang mit einer terroristischen Straftat oder einer anderen schweren Straftat steht, abgewendet werden muss, bearbeitet eine zentrale Zugangsstelle gemäß Artikel 29 Absatz 3 den Antrag unverzüglich und überprüft erst nachträglich, ob alle Voraussetzungen gemäß Artikel 32 erfüllt sind, einschließlich der Frage, ob tatsächlich ein Dringlichkeitsfall gegeben war. } } }

Alle Beschränkungen des Zugangs (etwa Art. 32) wiederholen lediglich die minimalsten Kriterien der Verhältnismäßigkeit. Es wirkt fast, als hätten die AutorInnen des Gesetzes versucht, hiermit die maximalen Rechte festzuschreiben, demit nicht nachher ein Gericht menschenrechtsfreundlichere Regelungen erkennt.

In der BRD sieht der Entwurf des EESDG folgende Behörden als benannt vor:

- die Bundespolizei,
- die sonstigen mit der Wahrnehmung grenzpolizeilicher Aufgaben betrauten Behörden,

- das Bundeskriminalamt und die Landeskriminalämter,
- die Zollfahndungsämter,
- das Zollkriminalamt,
- die mit der Steuerfahndung betrauten Dienststellen der Landesfinanzbehörden,
- die Verfassungsschutzbehörden des Bundes und der Länder,
- der Bundesnachrichtendienst,
- der Militärische Abschirmdienst

Weitere Behörden kann das BMI („Heimatministerium“) benennen. Immerhin muss eine Benennung durch den Bundesrat, so dass immerhin denkbar ist, dass jemand davon erfährt.

Im https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Taetigkeitsberichte/31TB_22.html | 31. TB des BfDI für 2022]] kritisiert dieser, dass ausgerechnet die Geheimdienste in dieser Liste nicht ganz verhältnismäßig wirken – was wohl unter <<Reinlink(gc/burger.html, Elend des bürgerlichen Datenschutzes)>> zu rubrizieren ist

= Technisches und Organisatorisches =

Das EES ist im Wesentlichen gebaut wie [\[\[SIS\]\]](#) und Freunde auch: [\[\[eu-LISA\]\]](#) betreibt ein Zentralsystem, das mit EDV-Systemen der nationalen Behörden synchronisiert wird (Art. 5). Hier ist die nationale Kontaktstelle laut EESDG aber das Bundesverwaltungsamt. Der zentrale Abgleich der Daten mit dem [\[\[VIS\]\]](#) war den Architekten des Systems wichtig. Wer den entsprechenden Art. 8 EESVO liest, muss sich fragen, warum die Systeme überhaupt getrennt aufgesetzt wurden.

Nicht Standardkost ist Artikel 13. Darin wird ein zentral betriebener „Web-Dienst“ postuliert, bei dem erfasste Menschen ihre Reisepläne eingeben können und dann erfahren, ob die Pläne Gesetzeskonform sind oder nicht. Und nicht nur die Betroffenen: In einer Art inversem [\[\[API\]\]](#) sollen auch Fluggesellschaften u.ä. auf diese Weise den Reisedatum abfragen können, wenn sie Name, Geburtsdatum, Dokumentnummer und Laufzeit des Reisedokuments eingeben.

= Geschichte =

Im <http://www.statewatch.org/news/2010/jul/eu-com-overview-information-management-com-385-10.pdf> | EU Overview Information Management]] von 2010 heißt es zum EES:

{ { { #!blockquote Noting that ‘overstayers’ constituted the largest group of irregular migrants in the EU, it suggested the possible introduction of an Entry/Exit System (EES) for third-country nationals entering the EU for short stays of up to three months. This system would record the time and place of entry and length of authorised stay and would transmit automated alerts to the competent authorities identifying individuals as overstayers. Based on biometric data verification, it would deploy the same biometric matching system and operational equipment as that used by SIS II and VIS. The Commission is currently conducting an impact assessment and, as stated in the Stockholm Programme Action Plan, will seek to present a legislative proposal in 2011. } } }

Nach etwas Diskussion (vgl. etwa <http://www.heise.de/tp/artikel/34/34932/1.html> | Telepolis vom 13.05.2011]]) brodelte der Kram dann lange Zeit vor sich hin und galt als Orwell-Monstrum, bis die Migrationshysterie von 2015f das Vorhaben wieder salonfähig machte.

2017 gab es dann eine „politische“ Einigung zwischen Rat und Parlament zu einer [\[\[http://www.statewatch.org/news/2017/sep/eu-entry-exit-system-consolidated-text-final-for-approval.pdf\]](http://www.statewatch.org/news/2017/sep/eu-entry-exit-system-consolidated-text-final-for-approval.pdf)Regelung für das EES]].

Im Oktober 2017 gab das EU-Parlament dazu aber grünes Licht.

In diesem Zusammenhang die die EU auch ein System namens ETIAS eingeführt, im Wesentlichen, um nach US-Vorbild Kreditkartennummern der Einreisenden abzugrasen.

Version #1

Erstellt: 2025-10-27 22:49:01 UTC von Datenschmutz Migration Bot

Zuletzt aktualisiert: 2025-10-27 22:49:01 UTC von Datenschmutz Migration Bot