VIS

<<TableOfContents>>

VIS ist eine Datenbank der [[Datenbanken EU|EU]], in der die Schengenstaaten Informationen über die von ihnen ausgestellten Visa austauschen, inklusive Fingerabdrücke der Antragsteller (Größenordnung: 20 Millionen Datensätze pro Jahr).

= Rechtsgrundlage =

VIS wird eingerichtet nach <<Doclink(2008-rat-vis.pdf,EU-Verordnung 767/2008)>>, hier bezeichnet als VISV.

Eine <<Doclink(2011-schild-visaverriss.pdf,Stellungnahme zur Visa-Warndatei von Hans-Hermann Schild)>> (Vorsitzender Richter am VG Wiesbaden), bemerkt zur nationalen Umsetzung:

{{{#!blockquote Eine entsprechende nationale Regelung, also mit den Worten des Bundesverfassungsgerichts: ein normenklares Gesetz, welches den einzelnen normenklar erkennen lässt, wer welche Daten über ihn hat, liegt nicht vor; zumindest habe ich hierzu nichts finden können. }}}

Vgl. auch [[http://europa.eu/legislation_summaries/justice_freedom_security/free_movement_of_persons_asylum_immigration/l14516_de.htm|europa.eu: Übersicht über die Rechtsakte zu VIS]]

== Grundsätzliches zur VIS-Verordnung ==

Grundsätzlich folgt VIS in vielem [[SIS]], insbesondere in der Struktur einer zentralen Datenbank, die national gespiegelt wird (VISV Art. 28). Allerdings scheint es, als sei bei VIS nur ein Übergabepunkt ("NI-VIS", national interface) definiert und die Systeme dahinter je nach Staat unterschiedlich (Art. 28 (4) VISV).

Hinter dem national interface sitzt eine nationale Kontaktstelle analog zu den SIRENEn. Offenbar waren die Erfahrungen mit Murks bei VISION so traumatisierend, dass Art. 26 (5) allerlei eigentlich selbstverständliche Forderungen an die nationalen Kontaktstellen formuliert ("back up and guarantee the continuous functioning").

VIS untersteht der [[Datenbanken EU|EU]]-Kommission (Art. 26 VISV).

== Art der Daten ==

Artikel 5 und 8-14 VISV regeln, welche Daten über die Menschen gespeichert werden sollen:

- Eine Antragsnummer (aus dem Visumsantrag), ggf. Visumnummer
- Statusinformation (Visum beantragt, erteilt, zuückgezogen, verweigert, verlängert)
- Stelle, die den Antrag angenommen bzw. das Visum erteilt, verweigert oder zurückgezogen hat
- ggf. Einlader``In: Name und Adresse
- Namen, Geschlecht, Geburtsdatum, Geburtsort (I)
- Beruf, Arbeitsstelle (etwa auch: Schule, Uni bei Schüler``Innen und Studis)
- Bei Minderjährigen Namen der Mutter und des Vaters (I)
- Nationalität, aktuell und bei der Geburt (I)
- Ausweispapiere mit Details zu Ausstellung und Gültigkeit (I)
- Visumtyp, Gebiet, für das das Visum gültig ist, Gültigkeit
- Reiseziel und -zweck, geplante Aufenthaltsdauer, Einreisedatum, Ausreisedatum
- Eintrittsort
- Wohnort (I)
- Fotografien (bereits bei der Antragstellung)
- Fingerabdrücke (bereits bei Antragstellung!)
- ggf. Verweigerungsgründe (z.B. gefälschte Papiere, Risiko illegaler Immigration, SIS-Ausschreibung, "[[Terrorlisten]]" usf).

Diese Daten ''müssen'' von den Behörden, die Visa ausstellen, in VIS eingegeben werden, und zwar für alle Mitreisenden (VISV, Art. 8).

Die Details der Fingerabdrücke lässt VISV Art. 9 offen; in der Praxis werden [[https://home-affairs.ec.europa.eu/policies/schengen-borders-and-visa/visa-information-system_en|nach Auskunft der Kommission]] alle zehn Finger gescannt, wenn sie sie kriegen können (pikanterweise überigens nicht von Regierungsmitgliedern anderer Staaten...).

== Zugriff ==

Zugriff haben sollen nach der EU-Komission die Visa, Asyl und Grenzkontrollbehörden der Länder. D.h in Deutschland dürften dieses die [[Datenbanken der Bundespolizei|Bundespolizei]] und das [[Datenbanken Bundesamt für Migration und Flüchtlinge|Bundesamt für Migration]] sein. Ob die europäische Grenzkontrollbehörde [[FRONTEX]] darauf Zugriff hat, ist nicht so klar.

Zugiff haben:

- die Visumbehörden der Mitgliedsstaaten (VISV, Art. 6, wobei Art. 15 noch sagt, welche Felder suchbar sein sollen); wenn VIS mal läuft, wird eine Liste der berechtigten Behörden veröffentlicht.
- die Grenzbehörden (Art. 18), die über Visumsnummer oder Fingerabdruck suchen und reglär Status, Fotos und Gültigkeitsdaten kriegen, aber Wunsch aber auch mehr.
- Polizeien im Schengeninneren (Art. 19); sie werden im Wesentlichen wie Grenzbehörden behandelt, nur, dass nicht vorgeschrieben ist, dass sie drei Jahre nach VIS-Start über Fingerabdrücke zugreifen ''müssen''.
- Asylbehörden suchen auch über Fingerabdrücke oder, wenn "the search with the fingerprints fail", mit fast allem anderen. Sie sollen so rauskriegen, wo jemand eingereist

ist und wer den "Fall an der Backe" hat (Art. 21), oder ob es einfache Gründe gibt, das Ayslverfahren gleich abzubrechen (Art. 22). Sie bekommen einfache Daten über eventuelle Visa zurück. Das ganze soll über die nationalen Zentralstellen laufen, es ist also offenbar erstmal nicht dran gedacht, dass die Asylbehörden direkten Zugriff auf VIS haben.
- Staatssicherheitsbehörden und Europol, wie in [[http://register.consilium.europa.eu/pdf/en/05/st15/st15142.en05.pdf|Beschlussvorlage 15142/05]] noch gefordert, sind erstmal nicht in der ursprünglich geplanten Form dabei; während viel noch von "innerer Sicherheit" abgedeckt ist, ist die alte "Schwerkriminalität" derzeit nicht abgedeckt.

Speicherfrist (ab letzter Änderung des Datensatzes) in VIS ist fünf Jahre (Art. 23); das ist keine Aussonderungsprüffrist, es muss also gelöscht werden. Ebenfalls gelöscht wird nach Einbürgerung (Art. 25).

VISV kennt umfangreiche Informationspflichten der Behörden gegenüber ihren Opfern (Art. 37: Information über Speicherung, ihren Zweck, das Auskunftsrecht usf). Das Auskunfts- und Berichtigungsrecht steht in Art. 38; merkwürdig ist die Regelung "Each Member State shall record any requests for such access." Was bedeutet das? Warum diese Regelung? An wen Auskunftsersuchen zu stellen sind, ist erstmal unklar, aber der BfDI wäre nach Art. 39 (2) wohl die erste Adresse. Er darf auch eine Kontrolle der Speicherungen aus der BRD vornehmen (Art. 41). Das ganze Ding hingegen soll nicht von einer JSB (wie bei SIS und Europol) begutachtet werden, sondern vom "European Data Protection Supervisor" (Art. 42).

Die Daten in VIS sollen zweckgebunden sein, können aber in andere Systeme kopiert werden (Art. 30), wenn diese den Zweck von VIS erfüllen. Angesichts von Zwecken wie "innere Sicherheit" dürfte das kein Hindernis sein. Auch an Drittstaaten können Daten übermittelt werden (Art. 31), allerdings nur die in der Liste oben mit I markierten Daten.

Zwecks der Datenschutzkontrolle sollen sämtliche Operationen an VIS mit Zweckbestimmung geloggt werden, also insbesondere auch Abfragen. Offenbar wollten die Gesetzesmacher dokumentieren, wie ernst sie es meinen (oder hatten wirklich keine Sorge, dass je wer nachguckt); jedenfalls sollen die Zugriffsprotokolle ein Jahr ''länger'' aufgehoben werden als die betreffenden Daten, was wohl die längste vorgeschriebene Speicherfrist für Log-Dateien überhaupt ist (Art. 34).

Die VISV ist insofern bemerkenswert, als Haftungsregeln in Art. 33 formuliert werden. Die sind zwar in der Regel kaum einklagbar, aber es sieht doch gut aus. Art. 36 betont nochmal, dass Missbrauch von VIS strafbar sein muss. Schade, dass das Papier den Streicherteppich dazu nicht hergibt.

VIS wird physikalisch in Straßburg stehen, mit einem Backup in Sankt Johann im Pongau/Österreich (VISV Art. 27); das deckt sich mit den Plänen für [[SIS II]].

== Geschichte ==

Nach 9/11 wollte der Rat eine Verschärfung der durch den Schengen-Acquis vorgeschriebenen gegenseitigen Konsultation in Visafragen über ein "Netzwerk" namens [[VISION]] (vgl. <<Ratsdokument(5148/02)>>). Dazu sollte eine Visa-Datenbank eingerichtet werden. Genauere

Pläne dafür wurden beim Sevilla-Gipfel 2002 geschmiedet, der <<Ratsdokument(2004/512)>> hat dann die VIS-Entwicklung in die Wege geleitet. Nach diesem Beschluss soll sich VIS in seiner Struktur eng an [[SIS]] anlehnen. Näheres zu VIS folgte dann 2005 in <<Ratsdokument(15142/05)>>.

Darin werden u.a. folgende Punkte festgehalten:

1. Die [[Staatsschutz]]-Behörden der Mitgliedsstaaten sollen auf jeden Fall Zugriff auf VIS haben.
2. [[Europol]] soll Zugriff auf VIS haben.
3. Aber natürlich nur, wenn es Anzeichen für Terrorismus gibt. VIS soll erstmal keine "regular crime fighting database" werden.

Zu diesem Zweck sollten Daten zu 20 Millionen Visa-Anträgen pro Jahr gespeichert werden, inklusive Fingerabdrücke. Bei einer Speicherfrist von fünf Jahren rechnete die Kommission mit 70 Millionen Fingerabdrucksätzen, die in VIS vorliegen sollen. Das Nehmen der Fingerabdrücken soll gemäß <<Ratsdokument(15142/05)>> unter Annahme der Unschuld der Opfer geschehen:

{{{#!blockquote individuals whose data are processed in the VIS [...] are to be treated as innocent individuals and not as suspects in a criminal investigation [...]

to lay down effective, proportionate and dissuasive sanctions to be imposed in case of infringement of data protection provisions, including criminal sanctions for particularly serious and intentionally committed infringements, }}}

Dieses soll durch einen jährlichen Audit unterstützt werden.

Parallel wurde am so genannten Schengen Border Code (SBC) gearbeitet, der 2006 als <<Ratsdokument(562/2006)>> verabschiedet wurde. Der SBC ist sozusagen das rechtliche Fundament für eine gemeinsame Grenzpolitik. Seit <<Ratsdokument(81/2009)>> hat die EU 2009 da auch die Verpflichtung reingeschrieben, VIS zu verwenden. Sie erlaubt aber, die Prüfung von Fingerabdrücken in der ersten drei Jahren von VIS mal kurz auszusetzen, wenn die Schlangen zu lang werden und sonst alles im grünen Bereich ist; vermutlich ist das die in Gesetzesform gegossene Erfahrung, dass solche Projekte, wenn sie überhaupt mal laufen, recht massive Kinderkrankheiten zeigen.

2008 verabschiedeten Rat und Parlament dann die <<Doclink(2008-rat-vis.pdf,Verordnung 767/2008)>>, die die Rechtsgrundlage von VIS darstellt.

2009 wird beschlossen, VIS von der [[http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52009PC0294:DE:HTML|IT-Agentur betreiben zu lassen]], die auch [[SIS]] betreiben soll.

Anlässlich des Innenministertreffens im Dezember 2009 hieß es VIS sollte Dezember 2010 an den Start gehen (vgl [[http://register.consilium.europa.eu/pdf/de/09/st16/st16883-re01.de09.pdf|Komissions-Mitteilung]] (S. 26).

Ende 2010 [[http://register.consilium.europa.eu/pdf/de/10/st15/st15427.de10.pdf|berichtet die Kommission ans EU-Parlament]] über die Ereignisse 2009 und ist immer noch optimistisch, den Kram 2010-12 an den Start zu kriegen. Offenbar hat die Entwicklung der nationalen Systeme gut geklappt, während beim Zentralen System, vor allem beim Biometrie-Matcher, Probleme auftraten. Insbesondere gingen Integrationstests schief, und zwar so drastisch, dass die Kommission Vertragsstrafen in Höhe von 7.6 ME verhängt hat.

Zur Sitzung der EU-Innenminister im Februar 2011 hat die Kommission die "Fertigstellung" von VIS für den 24.6.2011 (tatsächlich so genau) angekündigt.

Auch daraus wurde nichts, doch [[http://www.bmi.bund.de/SharedDocs/Pressemitteilungen/DE/2011/10/schengen.html|verkündete im Oktober 2011 das Bundesinnenministerium]] schließlich den Start von VIS.

Das allerdings war nur ein Start des "roll-out", und vermutlich funktionierte nicht viel. Jahre später berichtet die BfDI im <<Doclink(2015-bfdi-tb, 25. TB (2015))>>, S. 106, Ende 2015 seien dann auch die Konsulate in Russland und der Ukraine soweit -- ausgerechnet die Länder mit dem höchsten Visaaufkommen fehlten also bisher. Ebendort spricht die BfDI auch Zweifel aus, was den "flächendeckenden" Einsatz von "modernen Techniken und Verfahren zur Sicherstellung eines hohen Datensicherheitsniveaus" angeht.

Ebenfalls im <<Doclink(2015-bfdi-tb, 25. TB BfDI (2015))>>, S. 107 wird angesprochen, dass die Visavergabe häufig über externe Dienstleister erfolgt, also von den Betroffenen nicht direkt bei den Konsulaten betrieben wird, weil das idR zu mühsam und demütigend für Menschen mit Geld ist. Die VIS-Aufsichtsbehörde, findet, dass sie auch dabei auf ausreichenden Datenschutz aufpassen sollen dürfte.

Ein [[https://www.statewatch.org/news/2023/june/schengen-visas-private-contractors-follow-lax-approach-and-enjoy-wide-and-unmonitored-access-to-applicant-data/|Statewatch-Bericht im Juni 2023]] bietet einen weiteren Aspekt der haarigen Datenverarbeitung durch Dienstleister, in dem nämlich immer mehr Staaten fordern, Datenverarbeitung dieser Art habe im Land zu erfolgen:

{{{#!blockquote One concern is that data localization provisions in some countries, such as Russia and China, are increasingly strict and will “start applying to all private companies including external service providers, which are not protected by consular or diplomatic privileges.” The evaluation speculates that the continuation of current data practices could “provide a potential pathway for foreign governments to obtain access to the data of visa applicants to the EU.” }}}

== Zahlen ==

Zum [[http://dipbt.bundestag.de/dip21/btd/18/097/1809762.pdf|Stichtag 30. April 2016]] waren im VIS 24.727.407 Antragsdatensätze gespeichert.

Für 2022-12-31 nennt <<BtDS(20/5781)>> 55 471 638 Antragsdatensätze und atemberaubende 49 001 606 Fingerabdrücke. Diese Daten haben BRD-Behörden in fast 2000 Verfahren genutzt.

[[Datenbanken EU]]

Version #1
Erstellt: 2025-10-27 22:48:48 UTC von Datenschmutz Migration Bot
Zuletzt aktualisiert: 2025-10-27 22:48:48 UTC von Datenschmutz Migration Bot