

## Datenschutz im Visumverfahren

### Quellen:

Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung)

Verordnung (EG) Nr. 767/2008 (VIS-Verordnung)

Art. 11, 37, 48 Verordnung (EG) Nr. 810/2009 (Visakodex)

§§ 69 AufenthV

§§ 72a, 73 Abs. 1 und 3, 82, 86, 87, 88, 89, 89a, 90, 90c AufenthG

Ausländerzentralregistergesetz (AZRG)

AZRG-Durchführungsverordnung (AZRG-DV)

Visa-Warndatei-Gesetz (VWDG)

§§ 3, 78 ff. Bundesdatenschutzgesetz-neu (BDSG 2018)

### 1. Allgemeines

Die Verarbeitung personenbezogener Daten im Visumverfahren richtet sich nach der seit 25. Mai 2018 geltenden europäischen Datenschutz-Grundverordnung (DS-GVO), der VIS-VO, dem Visakodex, dem AufenthG, der AufenthV, dem AZRG, der AZRG-DV und dem VWDG. Die DS-GVO enthält für den öffentlichen Bereich weitreichende Öffnungsklauseln zugunsten nationaler Regelungen. Soweit ein Sachverhalt nicht durch die vorgenannten vorrangigen EU-Verordnungen abschließend geregelt ist, richtet sich der Datenschutz im Visumverfahren daher nach nationalen Spezialgesetzen (AufenthG, AufenthV, AZRG, AZRG-DV, VWDG) – ggf. in Verbindung mit den einschlägigen Vorschriften der DS-GVO – , und mangels spezialgesetzlicher Bestimmungen nach dem neu gefassten und ebenfalls am 25. Mai 2018 in Kraft getretenen Bundesdatenschutzgesetz-neu (BDSG 2018).

Für die Anforderungen an den Datenschutz spielt es keine Rolle, ob eine Datei lokal, z.B. in einer Auslandsvertretung, oder bundesweit geführt wird. Es gelten die gleichen Grundsätze (vgl. Art. 3 Abs. 1, Abs. 3 DS-GVO).

**Personenbezogene Daten** sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen, wobei ausreicht, dass eine Person indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der Identität dieser Person sind, identifiziert werden kann (vgl. Art. 4 Nr. 1 DS-GVO). Statistische Angaben fallen nicht hierunter.

Der Begriff der **Verarbeitung** im Sinne der DS-GVO erfasst jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang im Zusammenhang mit personenbezogenen Daten. Insbesondere sind erfasst das Erheben, Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, der Abgleich oder die Verknüpfung, die Einschränkung, das Löschen und die Vernichtung (vgl. Art. 4 Nr. 2 DS-GVO).

**Im Visumverfahren** findet die Verarbeitung personenbezogener Daten insbesondere statt bei der Eingabe von Daten in RK-Visa und im Rahmen der Aktenführung, aber auch bei der automatisierten Abfrage über das Bundesverwaltungsamt (BVA) sowie im Fall von Überprüfungen von Antragstellerangaben und ggf. der Übermittlung von Daten an Dritte.

## 2. Rechtliche Grundlagen

Der Datenschutz ist geleitet von den in Art. 5 DS-GVO niedergelegten Grundsätzen. Hierzu zählen insbesondere der Grundsatz der Rechtmäßigkeit (insbesondere keine Verarbeitung ohne Rechtsgrundlage, Art. 5 Abs. 1 lit. a) i.V.m. Art. 6 DS-GVO), der Grundsatz der Datenminimierung (Beschränkung auf das zum Zwecke der Verarbeitung notwendige Maß, Art. 5 Abs. 1 lit. c) DS-GVO) und der Grundsatz der Speicherbegrenzung (Identifizierbarkeit der betroffenen Person nur so lange, wie es für die Zwecke, für die die Daten verarbeitet werden, erforderlich ist, Art. 5 Abs. 1 lit. e)).

Nach dem im Datenschutzrecht geltenden „Verbot mit Erlaubnisvorbehalt“ **bedarf jeder Eingriff** in das informationelle Selbstbestimmungsrecht **einer Rechtsgrundlage** (Art. 6 Abs. 1 DS-GVO). Die Rechtmäßigkeit der Verarbeitung personenbezogener Daten ist zuerst nach der DS-GVO zu beurteilen. Im Bereich der öffentlichen Verwaltung lässt diese einen weiten Regelungsspielraum. Daher ist zu prüfen, ob es bereichsspezifisches Datenschutzrecht gibt. Ist dies nicht der Fall oder sind die bereichsspezifischen Vorschriften nicht abschließend, gilt ergänzend das BDSG 2018.

Über Art. 6 Abs. 2 und 3 i.V.m. Abs. 1 lit c) und e) DS-GVO sind insbesondere die im AufenthG und der AufenthV enthaltenen Spezialregelungen weiterhin anwendbar. Im nationalen Aufenthaltsrecht stellen die §§ 86-91g AufenthG und die Verordnungsermächtigungen in § 99 AufenthG i.V.m. § 69 AufenthV somit spezialgesetzliche Regelungen insbesondere für die Datenerhebung, -speicherung und -übermittlung durch die Auslandsvertretungen dar.

Ist keine spezielle Ermächtigungsgrundlage einschlägig, kommen die folgenden allgemeinen Ermächtigungen in Betracht, sofern die bereichsspezifischen Regelungen nicht abschließend sind:

- Art. 6 Abs. 1 lit. c) DS-GVO (rechtliche Verpflichtung der Auslandsvertretung), ggf. i.V.m. Art. 6 Abs. 2 DS-GVO in Verbindung mit nationalem Recht;
- Art. 6 Abs. 1 lit. e), Abs. 2 DS-GVO i.V.m. § 3 BDSG 2018 (Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder Ausübung öffentlicher Gewalt, die der Auslandsvertretung übertragen wurde); die zu erfüllende Aufgabe muss sich dabei aus den allgemeinen bzw. spezifischen Fachgesetzen ergeben.

## 3. Erhebung personenbezogener Daten durch die Auslandsvertretungen

Die Auslandsvertretungen gehören zu den gem. § 86 AufenthG mit der Ausführung dieses Gesetzes betrauten Behörden, die zum Zweck der Ausführung des AufenthG und ausländerrechtlicher Bestimmungen in anderen Gesetzen personenbezogene Daten erheben dürfen. Wichtig ist der korrespondierende Grundsatz in § 87 Abs. 1 AufenthG, wonach alle öffentlichen Stellen (mit Ausnahmen von Schulen sowie Bildungs- und Erziehungseinrichtungen) den in § 86 Satz 1 AufenthG genannten Behörden – und damit auch den Auslandsvertretungen – ihnen bekannt gewordene Umstände auf Ersuchen mitzuteilen haben, soweit dies für die dort genannten Zwecke erforderlich ist.

§ 69 AufenthV nennt die Daten, die im Rahmen des Visumverfahrens gespeichert werden dürfen, soweit dies für die Erfüllung der gesetzlichen Aufgaben der Auslandsvertretung

erforderlich ist. Die dort genannten Daten werden entsprechend in den Visumantragsformularen abgefragt und in RK-Visa eingegeben.

Über die in § 69 AufenthV genannten Daten hinaus ist es im Visumverfahren manchmal erforderlich (z.B. zur Überprüfung der Identität oder der Ehefähigkeit) zusätzliche Daten zu erheben bzw. Dokumente zu verlangen, sofern die Angaben des Antragstellers nicht anders überprüfbar sind. Die Datenerhebung darf nur erfolgen, soweit dies im Einzelfall zur Aufgabenerfüllung erforderlich ist, Art. 5 Abs. 1 lit. c) DS-GVO, § 86 Satz 2 AufenthG.

In jedem Fall **sind unnötige Doppelanforderungen oder die** (ggf. rein vorsorglich gedachte) **Erhebung überflüssiger Daten oder Urkunden unbedingt zu vermeiden**. Entsprechend sind bei Anhörungen/Interviews Fragen zum privaten Lebensbereich nur insoweit zu stellen, als sie zur Aufklärung des Sachverhalts erforderlich sind. Im Umkehrschluss sind Befragungen – einschließlich persönlicher Fragen – z.B. von Ehegatten **bei konkreten Verdachtsmomenten** auf eine Scheinehe zulässig (vgl. Beitrag „Ehegattennachzug“).

#### 4. Führen der Visadatei

##### a) **Visadatei:**

Gemäß § 69 AufenthV führen die Auslandsvertretungen eine automatisierte Datei über die **beantragten Visa**, sowie alle im Laufe des Verfahrens getroffenen Entscheidungen. Die genauere Auflistung der regelmäßig zu erfassenden Daten ergibt sich aus § 69 Abs. 2 AufenthV.

Die Verarbeitung personenbezogener Daten **bevor überhaupt ein Visumantrag gestellt wurde**, ist **grundsätzlich nicht zulässig**, da in diesen Fällen keine rechtliche Verpflichtung oder zu erfüllende öffentliche Aufgabe die Verarbeitung erforderlich macht und somit rechtfertigt. Dies gilt z.B. für Fälle, in denen andere Schengen-Vertretungen über potentielle Antragsteller informieren, die möglicherweise einen nicht rechtskonformen Antrag stellen werden. Auch andere Behörden oder Privatpersonen teilen ggf. schon vor Beantragung eines Visums mit, dass einer Person kein Visum erteilt werden sollte. Eine pro-forma-Speicherung in RK-Visa ist in diesen Fällen aus den genannten Gründen nicht zulässig.

Bei einem neuen Visumantrag (z.B. auf Erteilung eines Besuchvisums) einer Person, für die aufgrund eines früheren Visumantrags noch ein **laufendes Klageverfahren anhängig ist**, ist vor einer Entscheidung mit Referat 509 Rücksprache zu halten. Ein dann erteilter Hinweis von Referat 509, während eines laufenden Klageverfahrens kein Visum zu erteilen, ist unter dem Namen der betreffenden Person in RK-Visa einzugeben. Da zu der betreffenden Person aufgrund des streitigen Vorantrags bereits ein Datensatz besteht, ist die Speicherung insofern zulässig (ein neuer Datensatz für das Klageverfahren muss nicht erstellt werden).

##### b) **„Einladerdatei“:**

Besonders hervorzuheben ist die Zulässigkeit der Speicherung von Daten von Einladern an den Auslandsvertretungen. Gemäß § 69 Abs. 2 Nr. 2 lit. g) aa) AufenthV sind Name und Anschrift der bei der Beantragung benannten Referenzpersonen im Inland in die Visadatei aufzunehmen (also Name und Anschrift desjenigen, der *in Deutschland* eine

Verpflichtungserklärung abgegeben oder eine Einladung ausgesprochen hat bzw. vom Antragsteller als Referenzperson benannt wurde). Die „Einladerdatei“ ist somit praktisch keine neue oder eigene Datei, sondern Bestandteil der Visadatei an der Auslandsvertretung.

In RK-Visa werden die Daten strukturiert auf den Reitern 3 und 4 erfasst.

### c) **Visawarndatei:**

Es gilt der Grundsatz, dass eine **informelle „Visawarndatei“ nicht geführt werden darf**. Zulässig ist hingegen die **Visa-Warndatei nach dem Visa-Warndateigesetz (VWDG)**. Mit der Visa-Warndatei wird die Möglichkeit geschaffen, die an einem Visumantrag beteiligten Personen und Organisationen gezielt auf rechtswidriges Verhalten im Zusammenhang mit einem Visumverfahren oder mit sonstigem Auslandsbezug zu überprüfen.

In ihr werden Daten zu Personen gespeichert, die wegen einer für das Visumverfahren relevanten Katalogstraftat nach dem AufenthG oder dem Schwarzarbeitsbekämpfungsgesetz, oder bestimmten anderen Straftaten (Menschen- und Kinderhandel oder bestimmte Betäubungsmitteldelikte) rechtskräftig zu einer Geld- oder Freiheitsstrafe verurteilt worden sind (siehe § 2 Abs. 1 Nr. 1 VWDG). Darüber hinaus werden Warndaten gespeichert zu Visumantragstellern, die sich im Visumverfahren selbst rechtswidrig verhalten haben, sowie zu Einladern, Verpflichtungsgebern und Personen, die im Visumverfahren Bestätigungen abgegeben haben, wenn diese im Rahmen ihrer Erklärungen falsche Angaben gemacht haben oder – im Fall des Verpflichtungsgebers – ihrer Verpflichtung nicht nachgekommen sind. Siehe im Einzelnen VHB-Beitrag „*Visa-Warndatei*“.

Ein Gastgeber, der eine **Verpflichtungserklärung** gemäß §§ 66 bis 68 AufenthG abgegeben hat und diese **widerruft**, kann gemäß § 2 Abs. 2 Satz 1 VWDG in die Speicherung seiner Daten unabhängig von einem Visumverfahren einwilligen. Die Auslandsvertretungen werden in diesen Fällen oft gebeten, dafür Sorge zu tragen, dass ein Visum nicht erteilt wird. In diesen Fällen ist die Datenerfassung und Speicherung **ausnahmsweise zulässig, bevor ein Visumantrag gestellt wurde**. Zum Umfang der zulässigerweise zu erfassenden Daten siehe § 3 VWDG; insbesondere dürfen nur Angaben zum Verpflichtungsgeber gespeichert werden. Nicht zulässig ist die Speicherung personenbezogener Daten desjenigen, zu dessen Gunsten die Verpflichtung ausgesprochen wurde.

## 5. Informationspflichten

Art. 12 DS-GVO normiert Anforderungen an die Transparenz der Informationen, an die Kommunikation und die Modalitäten für die Ausübung der Rechte der betroffenen Person. Art. 13 f. DS-GVO sehen einen umfangreichen Katalog **proaktiver Benachrichtigungen** vor, wobei danach differenziert wird, ob die Daten bei der betroffenen Person erhoben werden (Art. 13 DS-GVO) oder nicht (Art. 14 DS-GVO). Dies betrifft unter anderem Kontaktdaten des Datenverarbeiters, die Verarbeitungszwecke sowie die Rechtsgrundlage, gegebenenfalls die Empfänger oder Kategorien von Empfängern der Daten sowie ggf. die Absicht der Übermittlung in ein Drittland, aber auch die Dauer der Speicherung, beziehungsweise die Kriterien für die Festlegung dieser Dauer. Der Betroffene ist zudem über seine Rechte zu informieren (siehe hierzu Ziffer 9).

Die Datenschutzinformation ist dem **Antragsteller spätestens bei der Einreichung des Antragsformulars in Papierform auszuhändigen**. Die Aushändigung sollte quittiert und die Quittierung zu den Akten genommen werden. Zudem sollte die Datenschutzinformation auf der Webseite der Auslandsvertretung an gut sichtbarer Stelle (am besten in unmittelbarer Nähe zu den Antragsformularen) zum Abruf zur Verfügung gestellt und in den Warteräumen (ggf. auch des externen Dienstleisters) an gut sichtbarer Stelle ausgehangen werden. Eine Musterinformation, die ggf. zu übersetzen, ortsangemessen anzupassen und ist, befindet sich in **Anhang I** zu diesem Beitrag.

Mit seiner Unterschrift unter dem Visumantragsformular für Schengen-Visa bestätigt der Antragsteller u.a., die am Ende des einheitlichen Antragsformulars (Anhang I zum Visakodex) aufgeführten **datenschutzrechtlichen Informationen zur Speicherung im Visa-Informationssystem** (VIS) und die Hinweise zu seinen Rechten gemäß der VIS-Verordnung zur Kenntnis genommen zu haben.

**Dritte, deren Daten im Visumverfahren verarbeitet werden** (z.B. Einlader, Personen, die für den Antragsteller eine Verpflichtungserklärung abgeben, Arbeitgeber von Antragstellern, deren Daten in den Antragsunterlagen enthalten sind), erhalten über die in Anhang I befindliche Musterinformation ebenfalls die Möglichkeit, Kenntnis über die Verarbeitung ihrer personenbezogenen Daten im Visumverfahren zu erlangen. Da hier oftmals kein direkter Kontakt zwischen der Auslandsvertretung und dem Dritten besteht, kommt der Möglichkeit der Einsichtnahme über die Webseite der Auslandsvertretung und durch Aushang in den Warteräumen besondere Bedeutung zu.

**Verpflichtungsgeber** werden zudem bei Abgabe ihrer Verpflichtungserklärung von der die Erklärung aufnehmenden Stelle datenschutzrechtlich informiert.

## **6. Datenübermittlung an inländische Behörden**

### **a) Automatisierte Datenweitergabe über das Bundesverwaltungsamt**

Die Auslandsvertretungen haben die für das Visumverfahren erforderlichen Daten elektronisch zur Verfügung zu stellen, um die **automatisierte Übermittlung an die im Visumverfahren zu beteiligenden Behörden** sicherzustellen, § 90c AufenthG. Dies gilt insbesondere auch für Daten zu Einladern, Verpflichtungsgebern und sonstigen Referenzpersonen (vgl. §§ 72a Abs. 1, 73 Abs. 1, und 4 AufenthG). Dies geschieht durch die Eingabe der erhobenen Daten in RK-Visa und die automatisierte Datenübermittlung über das BVA. Die Daten sind unverzüglich zu löschen, sobald die Bereitstellung für das Visumverfahren nicht mehr erforderlich ist; dies geschieht automatisiert ohne weitere Veranlassung durch die Auslandsvertretungen.

Die Auslandsvertretungen sind gemäß § 87 Abs. 2 Satz 1 Nr. 1 AufenthG verpflichtet, die **Ausländerbehörden** über den Aufenthalt eines Ausländers zu unterrichten, der keinen erforderlichen Aufenthaltstitel besitzt und dessen Abschiebung nicht ausgesetzt ist. Eine Unterrichtungspflicht besteht auch, sollte ein Verstoß gegen eine räumliche Beschränkung oder ein sonstiger Ausweisungsgrund festgestellt werden (§ 87 Abs. 2 Satz 1 Nr. 2 und Nr. 3). Ebenso sind personenbezogene Daten den zuständigen Ausländerbehörden zu übermitteln, soweit die Daten für die Durchsetzung der vollziehbaren Ausreisepflicht gegenüber dem

Ausländer von Bedeutung und für die Feststellung der Identität oder Staatsangehörigkeit geeignet sein können, § 87 Abs. 2 Satz 3 AufenthG.

§ 90 AufenthG enthält Unterrichtungspflichten gegenüber den **zuständigen Behörden** bei konkreten Anhaltspunkten **für Verstöße gegen arbeits-, sozialhilfe- und sozialversicherungsrechtliche Regelungen**. Neben der Zusammenarbeit mit den nach dem Schwarzarbeitsbekämpfungsgesetz zuständigen Behörden bildet die Norm die Rechtsgrundlage für Mitteilungen an Staatsanwaltschaften und Strafgerichte im Hinblick auf opferschutzrelevante Aufenthaltstitel.

Die Auslandsvertretungen arbeiten im Visumverfahren mit den **Sicherheitsbehörden** eng zusammen, soweit dies zur Erfüllung ihrer gesetzlichen Aufgaben erforderlich ist. Die Datenübermittlung richtet sich insoweit neben §§ 72a Abs. 1, 3 und 73 Abs. 1 AufenthG nach Art. 6 Abs. 1 lit c) und lit e), Abs. 2 DS-GVO i.V.m. §§ 25, 23 BDSG 2018. Personenbezogene Daten dürfen demnach an andere öffentliche Stellen im Inland weitergegeben werden, wenn dies zur Abwehr erheblicher Nachteile für das Gemeinwohl oder einer Gefahr für die öffentliche Sicherheit, die Verteidigung oder die nationale Sicherheit, zur Wahrung erheblicher Belange des Gemeinwohls oder zur Sicherung des Steuer- und Zollaufkommens (§ 23 Abs. 1 Nr. 3 BDSG 2018), zur Verfolgung von Straftaten oder Ordnungswidrigkeiten, zur Vollstreckung oder zum Vollzug von Strafen oder straf- oder jugendstrafrechtlichen Maßnahmen oder zur Vollstreckung von Geldbußen (Nr. 4) oder zur Abwehr einer schwerwiegenden Beeinträchtigung der Rechte einer anderen Person (Nr. 5) erforderlich ist.

#### **b) Datenübermittlung an den Bundesnachrichtendienst**

Maßgebliche Rechtsgrundlage ist das Gesetz über den **Bundesnachrichtendienst** (BNDG) i.V.m. mit dem Bundesverfassungsschutzgesetz. Diese Gesetze gehen insoweit als spezialgesetzliche Regelungen dem BDSG 2018 vor (§ 1 Abs. 2 BDSG 2018). Nach § 23 Abs. 3 des BNDG darf der BND „nach § 18 Abs. 3 des Bundesverfassungsschutzgesetzes jede Behörde um die Übermittlung der zur Erfüllung seiner Aufgaben erforderlichen Informationen einschließlich personenbezogener Daten ersuchen und nach § 18 Abs. 4 des Bundesverfassungsschutzgesetzes amtlich geführte Register einsehen, soweit es zur Erfüllung seiner Aufgaben erforderlich ist.“ Aufgrund dieser Regelung bestehen keine Bedenken, in begründeten Einzelfällen dem BND **auf entsprechendes Ersuchen** hin Daten bestimmter Betroffener zugänglich zu machen.

Gemäß § 23 Abs. 1 BNDG dürfen die Auslandsvertretungen zudem **von sich aus** dem BND die ihnen bekannt gewordenen Informationen einschließlich personenbezogener Daten übermitteln, wenn tatsächliche Anhaltspunkte dafür bestehen, dass die Übermittlung für dessen Eigensicherung nach § 2 Abs. 1 Nr. 1 BNDG oder im Rahmen von dessen Aufgaben (§ 1 Abs. 2 BNDG) zur Sammlung von Informationen über bestimmte Gefahrenbereiche (siehe § 5 Abs. 1 Satz 3 des Artikel 10-Gesetzes) erforderlich ist.

Zu einer regelmäßigen Auswertung einer Vielzahl von Visumunterlagen nicht näher konkretisierter Personen bieten nach Interpretation des Datenschutzbeauftragten die geltenden gesetzlichen Bestimmungen jedoch keine Handhabe. In Zweifelsfällen ist vorab Weisung von Referat 508 einzuholen.

c) Zur **Übermittlungspflicht im Rahmen von Vaterschaftsanfechtungsverfahren** siehe Ziffern 87.2.4 und 90.5 VwV-AufenthG.

## 7. Datenübermittlung an ausländische Stellen

### a) Gegenseitige Unterrichtung von Behörden der Schengen-Staaten

Mit dem Visakodex wurde die Visumpolitik gegenüber Drittstaaten weiter harmonisiert. Die Verpflichtung zur praktischen Zusammenarbeit vor Ort (Art. 48 Abs. 1 Visakodex) und damit auch die ständige gegenseitige Unterrichtung der Vertretungen der Schengen-Staaten über relevante Vorgänge schließt auch die **Datenübermittlung an eine Vertretung eines Schengen-Staates auf deren Ersuchen** als Aufgabe der deutschen Auslandsvertretung i.S.d. Art. 48 VK, Art. 6 Abs. 3 lit. a) DS-GVO ein. Der **Datenverkehr innerhalb der Mitgliedstaaten der Europäischen Union und mit den anderen Vertragsstaaten des EWR** im Anwendungsbereich des EU-Rechts ist datenschutzrechtlich so zu einzustufen wie die Datenübermittlung an inländische Behörden.

Auf die Einspeicherung der Antragsdaten bei Schengen-Visaanträgen in das schengenweite Visainformationssystem gem. VIS-Verordnung wird jeder Antragsteller bereits im Schengen-Visumantrag hingewiesen (s.o., Ziffer 5). Auch über die zugriffsberechtigten Stellen und die Löschrfrist wird dort vor Antragstellung informiert.

### b) Datenübermittlung an Drittstaaten oder internationale Organisationen

Vor Übermittlung personenbezogener Daten an Drittstaaten **außerhalb der EU/des EWR** oder an eine internationale Organisation ist zweistufig zu prüfen, ob die vorgesehene Datenübermittlung zulässig ist. Zunächst ist zu prüfen, ob die allgemeinen Rechtmäßigkeitsvoraussetzungen nach der DS-GVO für die Verarbeitung personenbezogener Daten vorliegen. Sodann ist zu prüfen, ob die spezifischen Anforderungen für die Übermittlung in Drittländer und an internationale Organisationen gem. Art. 44 ff. DS-GVO vorliegen.

Im Visumverfahren erhobene personenbezogene Daten dürfen in ein Drittland oder an eine internationale Organisation nur übermittelt werden, wenn die EU-Kommission festgestellt hat, dass ein Drittland oder eine internationale Organisation über ein angemessenes Schutzniveau verfügt (Angemessenheitsbeschluss, Art. 45 DS-GVO) oder wenn geeignete Garantien vorliegen und den betroffenen Personen durchsetzbare Rechte und wirksame Rechtsbehelfe zur Verfügung stehen (Art. 46 DS-GVO). Dies kann u.a. gewährleistet werden durch ein **rechtlich bindendes und durchsetzbares Dokument zwischen der Auslandsvertretung und der empfangenden Behörde oder öffentlichen Stelle des Gastlandes** (vgl. Art. 46 Abs. 2 lit. a) DS-GVO).

Die Datenschutz-Grundverordnung erlaubt darüber hinaus ausnahmsweise eine Datenübermittlung an Drittstaaten oder internationale Organisationen in bestimmten Sonderfällen (Art. 49 DS-GVO), insbesondere wenn die **Übermittlung aus wichtigen**

**Gründen des öffentlichen Interesses notwendig** ist (Art. 49 Abs. 1 Satz 1 lit. d) DS-GVO). Das öffentliche Interesse muss im Unionsrecht oder im nationalen Recht anerkannt sein (Art. 49 Abs. 4 DS-GVO). Auf eine **Einwilligung** können sich Behörden bei hoheitlichem Handeln dagegen **nicht** stützen (Art. 49 Abs. 1 Satz 1 lit. a), Abs. 3 DSGVO).

Bei der Frage, ob eine Datenübermittlung aus wichtigen Gründen des öffentlichen Interesses notwendig ist, muss geprüft werden, ob nicht die Interessen der betroffenen Person an dem Ausschluss der Verarbeitung überwiegen. Die Auslandsvertretung muss daher bei konkreten Anhaltspunkten für falsche oder unvollständige Angaben im Visumverfahren das öffentliche Interesse an einer rechtmäßigen Entscheidung über den Visumantrag gegen die schutzwürdigen Interessen der von erforderlichen Überprüfungen betroffenen Personen abwägen. **Insbesondere wenn konkrete Anhaltspunkte für den Verdacht vorliegen, dass im Visumverfahren eingereichte Unterlagen ge- oder verfälscht oder unecht sind**, dürften Auslandsvertretungen in der Regel unter Offenlegung personenbezogener Daten des Antragstellers Nachforschungen auch gegenüber ausländischen nicht-öffentlichen Stellen anstellen (Wertung des Art. 32 Abs. 1 lit. b) Visakodex bzw. § 54 Abs. 2 Nr. 8a) AufenthG).

**Sollten Dritte**, die im Rahmen von Überprüfungen um Auskunft zu bzw. Bestätigung der vom Antragsteller gemachten Angaben und eingereichten Nachweise gebeten werden, **die Auskunft mit Hinweis auf datenschutzrechtliche Vorgaben verweigern**, kann der in **Anhang II** zu diesem Beitrag befindliche Textbaustein zusammen mit dem Auskunftersuchen übersandt werden.

**Gerichtsurteile und behördliche Anordnungen von Drittstaaten**, mit denen von Auslandsvertretungen die Übermittlung oder Offenlegung personenbezogener Daten verlangt werden, dürfen (unbeschadet anderer Regelungen in Kapitel V der DS-GVO) nur anerkannt und vollstreckt werden, wenn sie auf einer internationalen Übereinkunft – zum Beispiel einem Rechtshilfeabkommen – beruhen.

Ist die **Übermittlung** an Stellen im Drittland in hier nicht geschilderten Fallkonstellationen **im Einzelfall oder in bestimmten Fallgruppen** (etwa bei Anfangsverdacht einer schweren oder systematisch/bandenmäßig begangenen Straftat) aus Sicht der Auslandsvertretung erforderlich, ist hierzu Rücksprache mit Referat 508 zu halten.

Zur Datenübermittlung an Dritte und Einlader, auch Bundestagsabgeordnete, vgl. den Beitrag *„Akteneinsicht und Auskünfte im Visumverfahren“*.

## 8. Rechte des Betroffenen

### a) Auskunftsrechte

Zu den Auskunftsrechten des Antragstellers im Falle einer AZR- bzw. SIS-Einspeicherung wird auf den Beitrag *„AZR/SIS/Geschützter Grenzfehndungsbestand – Einspeicherung von Antragstellern“* verwiesen.

Art. 15 DS-GVO regelt das Auskunftsrecht der Betroffenen. Die betroffene Person hat das Recht, eine Bestätigung zu verlangen, ob sie betreffende personenbezogene Daten verarbeitet werden. Ist dies der Fall, hat sie ein Recht auf Auskunft über diese Daten sowie über Informationen unter anderem über die Verarbeitungszwecke, Herkunft der Daten, Empfänger, über die Dauer der Speicherung sowie über ihre Rechte. In der Regel wird diesen



Anforderungen durch das Recht des Antragstellers auf **Einsicht in die Visumakten** hinreichend Rechnung getragen (siehe auch Beitrag „*Akteneinsicht und Auskünfte im Visumverfahren*“).

#### **b) Berichtigungs-, Vervollständigungs- und Einschränkungrechte**

Die betroffene Person hat das Recht, die **Berichtigung** sowie im Hinblick auf den Zweck der Datenverarbeitung die **Vervollständigung** sie betreffender unzutreffender personenbezogener Daten zu verlangen (Art. 16 DS-GVO). Diesem Erfordernis wird die Möglichkeit, während des Visumverfahrens und während des Remonstrationsverfahrens Antragsunterlagen nachzureichen, in der Regel gerecht werden.

Die betroffene Person kann in bestimmten Fällen auch die **Einschränkung der Verarbeitung** verlangen (Art. 18 DS-GVO) – zum Beispiel, wenn die Auslandsvertretung die Daten nicht mehr länger benötigt, die betroffene Person sie jedoch zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen benötigt oder die betroffene Person Widerspruch gegen die Verarbeitung eingelegt hat und noch nicht feststeht, ob die berechtigten Gründe der Auslandsvertretung für die Fortsetzung der Verarbeitung gegenüber denen der betroffenen Person überwiegen.

Die Auslandsvertretung muss grundsätzlich, falls sie personenbezogenen Daten an Dritte übermittelt hat, allen Empfängern der Daten jede **Berichtigung, Löschung oder Einschränkung der Verarbeitung mitteilen** (Art. 19 DS-GVO).

#### **c) Recht auf Löschung**

Gemäß Art. 17 DS-GVO kann der Betroffene die Löschung seiner personenbezogenen Daten verlangen. Solange allerdings die Mindestaufbewahrungsfristen der Art. 37 Abs. 3 Visakodex (Schengen-Visa) bzw. § 69 Abs. 3 AufenthV (nationale Visa) noch nicht überschritten sind, dürfte bezüglich der in der Visumakte bzw. -datei enthaltenen Daten der Löschrund des Art. 17 Abs. 1 lit. a) DS-GVO noch nicht einschlägig sein, bzw. Art. 17 Abs. 3 lit. b) dem Löschrund entgegenstehen. Daher ist Löschrundbegehren in den ersten zwei Jahren nach Entscheidung über den Visumantrag in der Regel nicht stattzugeben.