Selbsterklärung über die Umsetzung datenschutzrechtlicher und weiterer Maßnahmen für die Nutzung des SIS und der SIS-Kom

Hinweise zum vorliegenden Formular:

Das BVA realisierte die technische Anbindung der deutschen Ausländerbehörden (ABHen) (einschließlich der Bundespolizeibehörden, der Bayerischen Grenzpolizei, der Wasserschutzpolizei Hamburg und der Polizei beim Deutschen Bundestag in der Funktion als Ausländerbehörde), des Bundesamts für Migration und Flüchtlinge (BAMF), der berechtigten obersten Landesbehörden, des Auswärtigen Amts (AA), des Bundesamts für Auswärtige Angelegenheiten (BfAA) und der Auslandsvertretungen (AVen) an das erweiterte SIS im Bundeskriminalamt (BKA) durch eine im Registerportal BVA eingebettete Weboberfläche und in der Endausbaustufe eine SIS-Kundenschnittstelle zur Integration in die jeweiligen Fachverfahren der Nutzerbehörden. Dabei werden die Auskunfts- und Meldungsanfragen der Nutzerbehörden seitens BVA über eine technische Schnittstelle an das BKA weitergeleitet. Die Auskunfts- und Meldungsergebnisse von BKA werden über das BVA den Nutzerbehörden zur Verfügung gestellt. Bitte berücksichtigen Sie, dass im Rahmen der Abfrage des SIS sowie der Eingabe in das SIS das Behördenkennzeichen und die durchführende Person beim BKA protokolliert werden.

Zudem schreiben die EU-Verordnungen zum SIS in bestimmten Fällen Konsultationen, Treffermeldungen und den weiteren Austausch von Zusatzinformationen in Bezug auf SIS-Ausschreibungen vor. Vor diesem Hintergrund entwickelte das BVA eine Kommunikationsplattform, über die eine formularbasierte Kommunikation mit der SIRENE Deutschland möglich ist (die sogenannte SIS-Kom). Hierfür stellt das BVA den Nutzerbehörden ebenfalls eine im Registerportal BVA eingebettete Weboberfläche und in der Endausbaustufe eine SIS-Kom-Kundenschnittstelle zur Integration in die jeweiligen Fachverfahren der Nutzerbehörden bereit.

Behörden, die einen lesenden und/oder schreibenden Datenzugriff auf das SIS erhalten, sind zum Informationsaustausch mit der SIRENE-Deutschland verpflichtet. Folglich wird diesen Behörden auch generell ein Datenzugriff auf die SIS-Kommunikationsplattform (SIS-Kom) gewährt, um Nachrichten von der SIRENE Deutschland empfangen und Nachrichten an die SIRENE Deutschland versenden zu können.[1]

Die nachfolgenden Angaben dienen der Prüfung der Voraussetzungen für den Datenzugriff auf das SIS/die SIS-Kom und bilden somit die Basis für die Einräumung des Datenzugriffs. Im Sinne des Artikel 10 der EU-Verordnung 2018/1862 ist die Sicherheit der Daten aus dem SIS und der über die SIS-Kom ausgetauschten Nachrichten durch technische und organisatorische Maßnahmen hinreichend zu gewährleisten.

Die Verantwortung für die Zulässigkeit des einzelnen (lesenden bzw. schreibenden) Datenzugriffs trägt die abrufende bzw. die dateneingebende Behörde/Stelle. Bitte tragen Sie dafür Sorge, dass sämtliche Datenzugriffsvoraussetzungen zu jeder Zeit gegeben sind und die Grundsätze für den einzelnen Datenzugriff von Ihren Mitarbeitenden eingehalten werden. Auf die Einhaltung der für Sie geltenden Anforderungen an die Sicherheit der Datenverarbeitung gemäß DSGVO (Verordnung (EU) 2016/679, Datenschutz-Grundverordnung) und BDSG (Bundesdatenschutzgesetz) wird verwiesen.

Bitte machen Sie im Folgenden vollständige Angaben. Bei Rückfragen wenden Sie sich bitte an das zuständige Referat S I 5 a im Bundesverwaltungsamt unter der Mailadresse SIS@bva.bund.de.

[1] Hiervon ausgenommen sind die Bundespolizeibehörden, die Bayerische Grenzpolizei, die Wasserschutzpolizei Hamburg und die Polizei beim Deutschen Bundestag in ihrer Funktion als Ausländerbehörde.

1. Behördendaten

Behördenkennzeichen im Registerportal des BVA: _____
(soweit vorhanden)

Name und Kontaktdaten der Behörde

Name	_____
Postanschrift	_____
E-Mail-Adresse	_____
Telefonnummer	_____

Kontakt für mögliche Rückfragen:

Name	_____
E-Mail-Adresse	_____
Telefonnummer	_____

Name und Kontaktdaten des bzw. der behördlichen Datenschutzbeauftragten:

Name	_____
E-Mail-Adresse	_____
Telefonnummer	_____

2. Aufstellungsort

Aufstellungsort(e) der Arbeitsplatzrechner zur Nutzung des SIS/der SIS-Kom:
(bitte benennen Sie hier die Behördenstandorte, von denen aus SIS-/SIS-Kom-Datenzugriffe geplant sind)

_____
_____
_____
_____

Der Datenzugriff auf das SIS und die SIS-Kom im Rahmen des mobilen Arbeitens bzw. der Telearbeit ist unter folgenden Voraussetzungen zulässig:

- Verwendung von SINA-Notebooks (einschließlich Thin Client und vergleichbare Produkte) bzw. und ggfs. durch das BSI zugelassene Nachfolgeprodukte.
- Sicherheitsaspekte des mobilen Arbeitens bzw. Telearbeit sind über separate Verpflichtungserklärungen mit den betroffenen Beteiligten umfassend geregelt.
- Vorliegen angemessener technischer und organisatorischer Maßnahmen (wie z.B. sicheres Arbeitsumfeld, festgelegte Prozesse bei Verlust der SINA, Diebstahlsicherung).

3. Checkliste zur Umsetzung der nach Art. 24, 25 u. 32 DSGVO (ggf. i.V.m. § 64 Abs. 3 BDSG) erforderlichen technischen und organisatorischen Maßnahmen zur Sicherheit der Datenverarbeitung

Die Sicherheit der Daten aus dem SIS und der über die SIS-Kom mit SIRENE DE ausgetauschten Nachrichten wird gewährleistet durch die folgenden Maßnahmen:

1. Zutritts-/Zugangskontrolle

☐ Es erfolgt elektronische oder visuelle Hauseingangskontrolle.
☑ Die Büros sind abschließbar und können nur durch zugangsberechtigtes Personal betreten werden.
☑ Arbeitsplatzrechner, über die auf das SIS/die SIS-Kom zugegriffen wird, sind so aufgestellt, dass Unbefugte die Bildschirme nicht einsehen können.

Es bestehen Weisungen an die Mitarbeitenden,
☑ die SIS/SIS-Kom-Anwendung abzumelden, wenn sie nicht mehr benötigt wird.
☑ Besucher und nicht datenzugriffsberechtigte Beschäftigte in einem Büro mit Bildschirm nicht unbeaufsichtigt zu lassen bzw. Bildschirme gegen entsprechende, unbefugte Datenzugriffe stets zu sperren.
☐ Sonstige Maßnahmen:

---

2. Zugriffs-/ Speicher- und Benutzerkontrolle

Es bestehen schriftliche Weisungen an die Mitarbeitenden,
☑ ausschließlich anlassbezogene und zur Erfüllung der Aufgabe erforderliche Datenzugriffe auf das SIS/SIS-Kom zu tätigen.
☑ die besondere Sensibilität der SIS-/SIS-Kom-Daten bei ihrer Tätigkeit zu berücksichtigen.
☑ ausgedruckte SIS-/SIS-Kom-Daten vor unbefugtem Datenzugriff geschützt aufzubewahren (nach Verschlusssachenanweisung (VSA)).
☑ ausschließlich über eigene Benutzerkennungen auf das SIS/die SIS-Kom zuzugreifen.
☑ als Passwörter eine Zahlen- und Buchstabenkombination zu verwenden[2] und diese nicht im Browser zu speichern.
☑ verwendete Passwörter nicht schriftlich am oder in der Nähe des Arbeitsplatzes aufzubewahren.
☐ Sonstige Maßnahmen:

Berechtigungskonzept:

☑ Für Datenzugriffe auf das SIS/die SIS-Kom und die weitere Verarbeitung personenbezogener Daten aus den Anwendungen liegt ein entsprechendes Berechtigungskonzept vor. Hierbei wurden die Vorgaben der DSGVO und des BDSG – insbesondere zur Umsetzung der erforderlichen technischen und organisatorischen Maßnahmen – beachtet. Aus dem

[2] Es muss aus 8 bis 20 Zeichen bestehen. Es muss Werte aus den Kategorien Großbuchstaben, Kleinbuchstaben, Zahlen und Sonderzeichen enthalten. Es darf nicht den Vornamen, den Nachnamen, die E-Mail-Adresse oder den Benutzernamen des Benutzers enthalten. Es darf nicht mit den 10 zuletzt verwendeten Passwörtern übereinstimmen.

Berechtigungskonzept haben sich Profile mit einer Beschreibung der Aufgaben und Zuständigkeiten der Personen zu ergeben, die zum Zugriff auf die Daten sowie zu ihrer Eingabe, Aktualisierung, Löschung und Abfrage berechtigt sind. Diese Profile können unverzüglich zur Verfügung gestellt werden, z.B. um eine Anfrage der Aufsichtsbehörden nach Art. 10 Abs. 1 Buchstabe h) EU-Verordnung 2018/1862 zu beantworten. Das Berechtigungskonzept wird in regelmäßigen Abständen auf Aktualität überprüft.

Der Betrieb erfolgt über ein (externes) Rechenzentrum: ☑ Ja ☐ Nein

Die Anbindung erfolgt über ein (externes) Rechenzentrum: ☑ Ja ☐ Nein

Falls ja, sind Datenzugriffe auf SIS/SIS-Kom-Daten durch Mitarbeitende des Rechenzentrums:

- ☐ nicht vorgesehen und technisch ausgeschlossen.
- ☑ nicht vorgesehen, technisch jedoch möglich.
  - ☑ Es existieren Maßnahmen zur Überwachung des unberechtigten Datenzugriffs und deren Umsetzung wird proaktiv überwacht.
- ☐ entspr. vertraglicher Regelungen in bestimmten Fällen vorgesehen.
  - ☐ Ein entsprechendes Berechtigungs-/Zugriffskonzept unter Berücksichtigung des IT-Grundschutz-Bausteins des Bundesamts für Sicherheit in der Informationstechnik (BSI) OPS 1.1.2 (A7 Regelung der Administrationstätigkeit) liegt vor.
  - ☐ Es existieren Maßnahmen zur Überwachung des unberechtigten Datenzugriffs und deren Umsetzung wird proaktiv überwacht.
  - ☐ Mitarbeitende des Rechenzentrums haben keine Schreibrechte auf die SIS / SIS-Kom-Daten.

3. <u>Auftragskontrolle</u>

Sofern die Behörde / Stelle einen Auftragsverarbeiter ((externes) Rechenzentrum) im Einsatz hat, wird die Auftragskontrolle gewährleistet durch:

- ☐ Satzung
- ☑ Vertrag
- ☐ Sonstige Maßnahmen:

---

4. <u>Eingabekontrolle</u>

Werden für das SIS relevante Eingaben (Anfragedaten und Meldungsdaten) innerhalb der angebundenen Datenverarbeitungssysteme (Fachverfahren) protokolliert? Falls ja, dürfen keine aus dem SIS übermittelten Auskunftsdaten innerhalb der Fachverfahren protokolliert werden. Die Übernahme und Speicherung der SIS-Daten in das Fachverfahren bleiben davon unberührt.

- ☐ Ja
- ☑ Nein

Werden für SIS-Kom relevante Eingaben (mit SIRENE Deutschland ausgetauschte Nachrichten) innerhalb der angebundenen Datenverarbeitungssysteme (Fachverfahren) protokolliert?

- ☐ Ja
- ☑ Nein

Im Fall der Erhebung von Protokolldaten dürfen auf diese nur Berechtigte zum Zwecke des Datenschutzes, der Strafverfolgung und der Sicherstellung des Betriebs lesend zugreifen. Im Übrigen gelten die Bestimmungen des BDSG.

☐ Grundsätzliche Maßnahmen zur Absicherung bzgl. der Verwendung von Protokolldaten werden eingehalten. Dies beinhaltet die Einhaltung rechtlicher Rahmenbedingungen (IT-Grundschutz-Baustein des BSI OPS 1.1.5 A5) und Zugriffsschutz für Protokollierungsdaten (IT-Grundschutz-Baustein des BSI OPS 1.1.5 A 10)

☐ Sonstige Maßnahmen:

---

5. Verfügbarkeitskontrolle

☑ Sollte das genutzte Fachverfahren einer zeitweisen Störung unterliegen, sind die Mitarbeiter angewiesen, für diesen Zeitraum die vom BVA bereitgestellten Weboberflächen zu nutzen.

☐ Sonstige Maßnahmen:

---

6. Trennungskontrolle

☑ Innerhalb der angebundenen Datenverarbeitungssysteme (Fachverfahren) erfolgt eine Trennung zwischen Produktions- und Testumgebung.

☐ Sonstige Maßnahmen:

---

7. Übertragungs-/Transportkontrolle

☑ Einsatz von TLS1.2 oder einer aktuelleren Version zur sicheren Datenübertragung. [3]

☐ Sonstige Maßnahmen:

---

8. Datenträgerkontrolle

☑ Es werden keine SIS- / SIS-Kom-Daten auf mobilen Datenträger (USB-Stick, externe Festplatten usw.) physisch transportiert.

☐ Sonstige Maßnahmen:

---

[3] Entsprechend der Empfehlungen des Bundesamts für Sicherheit in der Informationstechnik ist der Einsatz von TLS 1.2 oder einer aktuelleren Version vorzusehen (vgl. www.bsi.bund.de). Das Bundesverwaltungsamt behält sich daher vor, nicht mehr empfohlene Protokolle und Ciphers für die Nutzung des Registerportals abzuschalten.

9. Zuverlässigkeit und Datenintegrität

☑ Innerhalb der angebundenen Datenverarbeitungssysteme (Fachverfahren) werden die unter Punkt 4 genannten Maßnahmen eingehalten.

☐ Sonstige Maßnahmen:

---

4. Berücksichtigung weiterer Maßnahmen

Mit Ihrer untenstehenden Unterschrift bestätigen Sie zugleich die Einhaltung der folgenden Punkte:

1. Die Mitarbeitenden bzw. Endnutzer werden von den jeweils zuständigen Mitarbeitenden in meiner Behörde über ihre Pflichten unmittelbar informiert. Hierzu zählt z. B. die Ermächtigungsgrundlage bei der Eingabe einer Ausschreibung im SIS, beim Stellen der Anfrage an das SIS, aber auch bzgl. des Austauschs von Zusatzinformationen mit SIRENE Deutschland zu SIS-Ausschreibungen.

2. **Für die Nutzung von angebundenen Datenverarbeitungssystemen (behördeneigene Fachverfahren) gilt:**

   a) Die Einbindung der vom BVA bereitgestellten Kundenschnittstellen für SIS/SIS-Kom erfolgt gemäß der vom BVA bereitgestellten fachlichen und technischen Schnittstellenbeschreibung. Alle Daten einer Ausschreibung im SIS, einschließlich der Fehler- und Hinweismeldungen, müssen über das Fachverfahren dem Mitarbeitenden bzw. Endnutzer angezeigt werden. Alle Funktionen der Kundenschnittstellen müssen im Fachverfahren unterstützt werden und den Mitarbeitenden bzw. Endnutzer in geeigneter Weise zur Verfügung gestellt werden. Falls dies nicht oder nur teilweise der Fall ist, ist die Weboberfläche des Registerportals BVA für die nicht abgebildeten Anwendungsfälle zu verwenden. Dies gilt analog auch für die SIS-Kom. Sollten die Fachverfahren einer zeitweisen Störung unterliegen, sind für diesen Zeitraum ebenfalls die vom BVA bereitgestellten Weboberflächen zu nutzen.

   b) Es wird gewährleistet, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können.

   c) Meine Behörde verpflichtet sich, dafür Sorge zu tragen, dass bei Umstellungsarbeiten oder zur Qualitätssicherung, entsprechende Tests und Abnahmeprozesse in den behördeneigenen Fachverfahren erfolgen.

5. Unterschrift

Die genannten Maßnahmen zur Sicherheit der Datenverarbeitung sowie die weiteren Maßnahmen werden getroffen und eingehalten.

.....

Datum, Name, Unterschrift des Vertreters bzw. der Vertreterin der antragstellenden Behörde

.....

Datum, Name, Mitzeichnung des bzw. der behördlichen Datenschutzbeauftragten