

Darum geht es

Im Rahmen der Schengener und der Dubliner Zusammenarbeit werden zwischen den Behörden der beteiligten Staaten regelmässig Daten über Personen und Sachen ausgetauscht. Im Bereich von Schengen geschieht dies primär im Rahmen des so genannten Schengener Informationssystems (SIS; siehe auch Faktenblatt 6), einem elektronischen Fahndungssystem für gesuchte oder unerwünschte Personen sowie für gesuchte Gegenstände (Fahrzeuge, Waffen und dergleichen). Im Bereich von Dublin betrifft dies insbesondere die computergestützte zentrale Datenbank Eurodac (siehe auch Faktenblatt 5), in welcher die Fingerabdruckdaten aller Asylbewerber und illegal anwesenden Personen aus Drittländern erfasst werden. In diesem Zusammenhang stellen sich Fragen des Datenschutzes. Ziel ist, bei der Verarbeitung persönlicher Daten die Grundrechte und insbesondere die Privatsphäre der Betroffenen durch klare rechtliche Vorgaben zu schützen.

Der Missbrauch persönlicher Daten wird durch klare rechtliche Vorgaben verhindert

Das regelt Schengen/Dublin

Sowohl das Schengener Durchführungsübereinkommen (SDÜ) als auch die Dubliner Verordnung (Dublin II; diese ersetzt das Dubliner Übereinkommen) und die Verordnung zu Eurodac enthalten spezielle Datenschutzvorschriften. Diese regeln den Datentransfer im Rahmen der Schengener beziehungsweise Dubliner Zusammenarbeit. In weiten Teilen von Schengen/Dublin kommt daneben auch die allgemeine EG-Datenschutzrichtlinie (95/46/EG) zur Anwendung.

Für den Schengen- und Dublin-Bereich gelten jeweils spezielle Datenschutzvorschriften

Die wichtigsten Regeln, welche für den gesamten Informationsaustausch unter Schengen/Dublin gelten, sind die folgenden:

- Es dürfen nur bestimmte Daten ausgetauscht werden. Von einer im SIS ausgeschriebenen Person dürfen zum Beispiel neben den Personalien (inklusive besondere unveränderliche physische Merkmale) grundsätzlich nur der Ausschreibungsgrund, die zu ergreifende Massnahme sowie allenfalls der Hinweis «bewaffnet» oder «gewalttätig» registriert werden. Im Eurodac dürfen von den Asylsuchenden beziehungsweise illegal anwesenden Drittausländern neben den Fingerabdruckdaten grundsätzlich nur der Mitgliedstaat, der die Daten übermittelt hat, Ort und Zeitpunkt der Stellung des Asylantrags beziehungsweise des Aufgreifens sowie das Geschlecht gespeichert werden.

- Die Daten sind nur einem beschränkten Kreis von Personen zugänglich.
Für das SIS umfasst dieser Kreis alle behördlichen Stellen, welche für die Grenzkontrollen oder für sonstige polizeiliche und zollrechtliche Überprüfungen im Inland zuständig sind. Zu Daten von Drittausländern, welche zur Einreiseverweigerung ausgeschrieben sind, haben zudem die Behörden Zugang, die für die Erteilung von Visa und Aufenthaltstiteln zuständig sind (z.B. die Konsulate).
Die Eurodac-Datenbank wird von einer bei der EG-Kommission eingerichteten Zentraleinheit betrieben. Auf Anfrage eines Mitgliedstaates hin gibt sie Auskunft darüber, ob eine bestimmte Person im Eurodac registriert ist oder nicht. Die Mitgliedstaaten, welche die einzelnen Daten geliefert haben, behalten den Zugriff auf die gelieferten Daten und tragen die Verantwortung für deren Bestand und Richtigkeit.
- Die Daten dürfen nur zu den vorgesehenen Zwecken verwendet werden.
- Die Daten müssen richtig und aktuell sein.
- Die Daten dürften nur für eine limitierte Zeit aufbewahrt und müssen danach wieder gelöscht werden.
- Die betroffenen Personen haben ein Recht auf Auskunft sowie auf Überprüfung der Richtigkeit und auf allfällige Berichtigung oder Löschung der über sie gespeicherten Daten.
- Unabhängige Kontrollstellen haben dafür zu sorgen, dass die Datenschutzvorschriften eingehalten und die Rechte der Betroffenen nicht verletzt werden.
- Für den nationalen Teil des SIS (N-SIS) muss eine unabhängige nationale Kontrollinstanz bezeichnet werden. Für die zentrale SIS-Stelle in Strassburg (C-SIS) gibt es eine gemeinsame Kontrollinstanz.
- Für den rechtmässigen Betrieb von Eurodac ist die EG-Kommission zuständig.

Das sind die Auswirkungen auf die Schweiz

Die Schweiz erfüllt auf Bundesebene bereits heute grundsätzlich die Anforderungen, welche Schengen/Dublin (inklusive EG-Datenschutzrichtlinie) im Bereich des Datenschutzes stellen. Im Bereich Schengen wird neu insbesondere ein nationaler Bestandteil des SIS (N-SIS) bereitgestellt und dieses mit den in der Schweiz bereits bestehenden Datenaustauschsystemen verbunden. Dafür braucht es eine formell-gesetzliche Grundlage. In jenen Bereichen, in denen die Kantone von Schengen/Dublin direkt betroffen sind, sind – soweit nicht bereits vorhanden – entsprechende rechtliche Grundlagen zu erlassen. Im Übrigen muss jeder Kanton über eine unabhängige Kontrollinstanz verfügen.

Das Datenschutzrecht des Bundes ist mit Schengen/Dublin kompatibel; auf kantonaler Ebene werden punktuelle Anpassungen notwendig