

Sachdokumentation:

Signatur: DS 1655

Permalink: www.sachdokumentation.ch/bestand/ds/1655



Nutzungsbestimmungen

Dieses elektronische Dokument wird vom Schweizerischen Sozialarchiv zur Verfügung gestellt. Es kann in der angebotenen Form für den Eigengebrauch reproduziert und genutzt werden (private Verwendung, inkl. Lehre und Forschung). Für das Einhalten der urheberrechtlichen Bestimmungen ist der/die Nutzer/in verantwortlich. Jede Verwendung muss mit einem Quellennachweis versehen sein.

Zitierweise für graue Literatur

Elektronische Broschüren und Flugschriften (DS) aus den Dossiers der Sachdokumentation des Sozialarchivs werden gemäss den üblichen Zitierrichtlinien für wissenschaftliche Literatur wenn möglich einzeln zitiert. Es ist jedoch sinnvoll, die verwendeten thematischen Dossiers ebenfalls zu zitieren. Anzugeben sind demnach die Signatur des einzelnen Dokuments sowie das zugehörige Dossier.



Fakten statt Mythen Nr. 127 – 31. Mai 2018

Der gläserne Flüchtling: Datenschutz im Asylbereich

Von Nula Frei, Oberassistentin am Institut für Europarecht der Universität Fribourg

Wer diese Zeilen liest, musste mit Sicherheit in den letzten Wochen unzählige Male Datenschutz-Aktualisierungen akzeptieren und Newsletter-Einstellungen bestätigen. Dahinter steckt die neue [Datenschutz-Grundverordnung der EU](#) (DSGVO), die seit letzter Woche gilt. Diese Verordnung ist das derzeit fortschrittlichste Datenschutz-Instrument der Welt; sie stärkt die Rechte der Betroffenen und erweitert die Pflichten der Datenbearbeitenden.

Hohe Datenschutzstandards

Gemäss der DSGVO dürfen Daten nur bearbeitet (also gesammelt, gespeichert, aufbewahrt, verwendet, weitergegeben, archiviert, gelöscht etc.) werden, wenn die betroffenen Personen einwilligen, wenn ein Gesetz dies erlaubt oder wenn ein anderer wichtiger Grund besteht. Daten dürfen weiter nur zu dem Zweck bearbeitet werden, für den sie erhoben wurden (Grundsatz der Zweckbindung), es dürfen nur so viele Daten bearbeitet werden wie für den jeweiligen Zweck notwendig ist (Verhältnismässigkeit und Datenminimierung) und die betroffene Person muss sehen können, welche Daten, durch wen, wie und zu welchem Zweck bearbeitet werden (Grundsatz der Transparenz). Sie kann auch verlangen, dass falsche Daten über sie berichtigt oder gelöscht werden, selbst wenn die Daten bereits im Internet verbreitet worden sind (das berühmte [Recht auf Vergessenwerden](#)). Für sensible Daten, zum Beispiel Daten über die Gesundheit, die politischen oder religiösen Ansichten, die sexuelle Orientierung, Strafakten oder Sozialhilfebezug, bestehen erhöhte Anforderungen.

Und bei Asylsuchenden?

Ob Asylsuchende in letzter Zeit wohl auch E-Mails mit der Bitte um Einwilligung in die Aktualisierung der Datenschutzerklärungen für das Asylverfahren erhalten haben? Kaum. Das liegt erstens daran, dass die Datenbearbeitung im Asylbereich sich nicht auf die Einwilligung der Betroffenen, sondern auf eine gesetzliche Grundlage stützt. Zweitens ist die DSGVO in der Schweiz nicht anwendbar, jedenfalls nicht im Asylbereich.

Im Asylbereich ist das Schweizerische [Datenschutzgesetz](#), welches derzeit [revidiert](#) wird, sowie das [Asylgesetz](#) und weitere Verordnungen massgeblich. Die dort verankerten Grundsätze gleichen (im Ansatz) denen der DSGVO. Das ist auch wichtig, denn: Im Asylbereich werden in grossem Stil Personendaten bearbeitet. Das Staatssekretariat für Migration (SEM) unterhält mehrere Datenbanken, in denen Personendaten erfasst sind, mit klingenden Abkürzungen wie ZEMIS, Finasi, MIDES, AURORA und DOPO. Hinzu kommen Europäische Systeme wie Eurodac.

Weitgehende Zugriffsrechte auf Informationssysteme

In diesen Systemen werden Personendaten wie Name, Geburtsdatum, Geburtsort, Geschlecht, Staatsangehörigkeit, Adressen, Fingerabdrücke, Fotografien, Angaben über

den Gesundheitszustand oder Angaben über strafrechtliche Verfahren gespeichert. Die gesamten Akten des Asylverfahrens, also etwa auch Anhörungsprotokolle, werden dort ebenfalls verwaltet.

Ein Blick in die [Regelung dazu](#) zeigt, wer alles Zugriff auf dieses System hat: Die kantonalen und kommunalen Ausländerbehörden, die Polizeibehörden, Asyl- und Flüchtlingskoordinationsstellen und Arbeitsmarktbehörden, mehrere Stellen des fedpol, die Bundeskriminalpolizei, mehrere Stellen im Bundesamt für Justiz, das Bundesverwaltungsgericht, die kantonalen Grenzposten und das Grenzwachtkorps, die eidgenössische Finanzkontrolle, die Zentrale AHV-Ausgleichsstelle, die kantonalen Steuerbehörden, die Zivilstandsämter, der Nachrichtendienst des Bundes, die Eidgenössische Steuerverwaltung, die eidgenössische Zollverwaltung, die schweizerischen Auslandvertretungen und Missionen, mehrere Stellen im Eidgenössischen Departement für auswärtige Angelegenheiten (EDA). Zudem kann auch Dritten, welche Aufgaben im Asylbereich übernehmen, z.B. Betreibern von Unterkünften, Zugriff gewährt werden.

Eine sehr grosse Zahl von Behörden und Privaten hat also Zugriff auf teilweise sehr sensible Daten von Asylsuchenden. Dies ist in anderen Ländern sowie in den grossen Informationssystemen der EU zu beobachten. Im Zeitalter der Terrorismusbekämpfung wird ohnehin immer selbstverständlicher gefordert, dass die Datenbanken verknüpft sowie die Zugriffsrechte für Polizei, Staatsanwaltschaften und Geheimdienste erweitert werden. So [will die Schweiz](#) neuerdings auch den Strafverfolgungsbehörden Zugriff auf die in der Eurodac-Datenbank gespeicherten Fingerabdrücke von Asylsuchenden gewähren. Die EU-Kommission will mit der Begründung «Mehr Sicherheit durch Schliessen von Informationslücken» die EU-Visumsdatenbank VIS so [umbauen](#), dass alle Visumanträge automatisch mit sämtlichen anderen EU-Informationssystemen für Sicherheit und Migration abgeglichen werden.

Mehr Sicherheit durch Schwächung des Datenschutzes?

Zweifellos ist behördlicher Informationsaustausch für die Terrorismusprävention wichtig. Aber es erscheint doch fraglich, ob den Datenschutzgrundsätzen immer genug Rechnung getragen wird. Ist es wirklich verhältnismässig, dass eine derart grosse Zahl von Behörden und privaten Stellen die Daten jedes Asylsuchenden einsehen können? Ist es mit dem Zweckbindungsgrundsatz vereinbar, dass Daten wie Fingerabdrücke, die ursprünglich ausschliesslich für die Zuständigkeitsbestimmung im Asylverfahren erhoben wurden, später auch von den Strafverfolgungsbehörden abgeglichen werden können? Wird diese weitgehende Verwendung ihrer Daten den Asylsuchenden transparent gemacht? Und falls nicht: Besteht die Gefahr, dass Asylsuchende, die über diese weitgehende Verwendung informiert sind, weniger Informationen über ihre Gesundheit oder sexuelle Orientierung preisgeben, mit entsprechend negativen Folgen für ihr Asylgesuch?

Der gläserne Flüchtling

Das Szenario des «[gläsernen Bürgers](#)» ist bei Asylsuchenden also nicht so weit hergeholt. Der «gläserne Flüchtling» ist nicht mehr weit entfernt: Während für «normale Bürger» der Trend hin zu einer Stärkung des Datenschutzes geht, wird er im Bereich der Migrationskontrolle für Asylsuchende sukzessive geschwächt.