

UNHCR-Stellungnahme

**Zur Parlamentarischen Initiative 17.423:
Mitwirkungspflicht im Asylverfahren. Über-
prüfungsmöglichkeit bei Mobiltelefonen.
Vorentwurf und erläuternder Bericht der
Staatspolitischen Kommission des Natio-
nalrates vom 14. Februar 2020**

Juni 2020

Inhaltsverzeichnis

Inhaltsverzeichnis	2
1. Einleitung	3
2. Vorentwurf SPK-N	4
3. Völkerrechtliche Vorgaben	5
4. Kommentare zum Vorentwurf SPK-N	6
5. Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter (EDÖB)	12
6. Zusammenfassung der Empfehlungen	13

1. Einleitung

UNHCR bedankt sich für die Möglichkeit zum Vorentwurf der Staatspolitischen Kommission des Nationalrates (SPK-N) zur Änderung des Asylgesetzes und des Ausländer- und Integrationsgesetzes Stellung nehmen zu können. Ziel des Vorentwurfs ist die Umsetzung der Parlamentarischen Initiative 17.423 zur «Mitwirkungspflicht im Asylverfahren. Überprüfungsmöglichkeit bei Mobiltelefonen».¹

Vorgeschlagen wird, die Mitwirkungspflicht von Asylsuchenden durch die Verpflichtung zur Aushändigung von elektronischen Datenträgern zu erweitern, wenn deren Identität, Nationalität oder Reiseweg weder gestützt auf Identitätspapiere noch mit zumutbarem Aufwand auf andere Weise festgestellt werden kann. Gleichzeitig wird das SEM ermächtigt, zum Zweck der Abklärung von Identität, Nationalität oder Reiseweg die Daten, einschliesslich solcher, die nach dem Datenschutzgesetz als besonders sensibel eingestuft sind, auszuwerten.

UNHCR anerkennt grundsätzlich das legitime Interesse von Staaten, Personen auf ihrem Hoheitsgebiet zu identifizieren und sicherzustellen, dass bei Entscheidungen über Schutzersuchen auf umfassende und aktuelle Informationen zurückgegriffen werden kann. Der Zugriff auf persönliche Daten stellt jedoch ein wesentliches Element des Rechts auf Privatsphäre dar und ist ein weitreichender Eingriff in dieses völker- und verfassungsrechtlich geschützte Recht (sowie in andere Menschen- und Grundrechte), der nur unter engen Voraussetzungen zulässig ist. UNHCR hält es für grundsätzlich möglich, einen Zugriff so auszugestalten, dass er die völker- und verfassungsrechtlichen Voraussetzungen erfüllt. Der vorliegende Gesetzesentwurf erfüllt diese Voraussetzungen jedoch noch nicht ausreichend. UNHCR erachtet es für unerlässlich, dass in einem formellen Gesetz präzise Rahmenbedingungen für die Möglichkeit der Bearbeitung persönlicher Daten geschaffen werden, welche den übergeordneten Grundsätzen der Rechtmässigkeit, der Notwendigkeit und der Verhältnismässigkeit - beziehungsweise den entsprechend in der Schweizer Bundesverfassung genannten Einschränkungsvoraussetzungen von Grundrechten - genügen.

UNHCR legt daher – auf Grundlage seines völkerrechtlichen Mandats² – die folgenden ausgewählten und nicht abschliessenden Empfehlungen zum vorliegenden Vorentwurf vor.

¹ 17.423 *Parlamentarische Initiative, Mitwirkungspflicht im Asylverfahren, Überprüfungsmöglichkeit bei Mobiltelefonen, Vorentwurf und erläuternder Bericht der Staatspolitischen Kommission des Nationalrates*, 14. Februar 2020, abrufbar unter: https://www.admin.ch/ch/d/gg/pc/documents/3111/AsylG_Mitwirkungspflicht_Bericht_de.pdf [zuletzt besucht am 21.05.2020].

² Siehe insbesondere Art. 35 des Abkommens von 1951 über die Rechtsstellung der Flüchtlinge (GFK); Art. II Protokoll über die Rechtsstellung der Flüchtlinge von 1967, S. 1, abrufbar unter: <http://www.unhcr.org/3b66c2aa10> (2.5.2018); Satzung des Amtes des Hohen Kommissars der Vereinten Nationen für Flüchtlinge, Resolution 428 (V) der UN-Generalversammlung, Annex, UN Doc. A/1775, 1950.

UNHCR hofft, dass diese im weiteren Prozess berücksichtigt werden und steht für Rückfragen gerne zur Verfügung.

2. Vorentwurf SPK-N

Die Vorlage der SPK-N ermächtigt die Behörden gemäss erläuterndem Bericht den Zugriff auf mobile Datenträger zwecks Auswertung von Personendaten, wenn die Identität, die Nationalität oder der Reiseweg der Schutzsuchenden weder aufgrund von Identitätspapieren noch mit zumutbarem Aufwand auf anderem Weg festgestellt werden kann. Damit soll «sichergestellt werden, dass das Recht auf Asyl jenen Menschen erteilt wird, die diesen Schutz auch wirklich benötigen.»³ Der Zugriff soll durch eine entsprechende Erweiterung der in Art. 8 Asylgesetz geregelten Mitwirkungspflicht der Asylsuchenden erfolgen.

Dabei sind folgende Massnahmen vorgesehen:

- Verpflichtung der Asylsuchenden, elektronische Datenträger (Mobiltelefone, Computer, Speichermedien wie USB-Sticks etc.) auszuhändigen (nArt. 8 Abs. 1 lit. g AsylG);
- Ermächtigung des SEM diese während der Dauer des Asylverfahrens zu bearbeiten. Dies schliesst ein: Auslesen von Daten; Zwischenspeicherung; Auswertung und Verwendung der Daten; Ablegen der ausgewerteten Daten im Asylossier (nArt. 8a Abs. 1 – 6 AsylG).

Im Rahmen des Wegweisungsverfahrens sind zudem folgende Massnahmen vorgesehen:

- Aushändigung elektronischer Datenträger und Auswertung der Personendaten sinngemäss zu nArt. 8a AsylG, sofern die Identität nicht feststeht und gültige Reisepapiere nicht mit zumutbarem Aufwand auf andere Weise beschafft werden können (nArt. 47 AsylG).

Für die Bearbeitung von Personendaten verweist der Vorentwurf (nArt. 8a AsylG) auf das Bundesgesetz über den Datenschutz⁴. Demnach versteht man unter «Bearbeiten» «jeden Umgang mit Personendaten, unabhängig von den angewandten Mitteln und Verfahren, insbesondere das Beschaffen, Aufbewahren, Verwenden, Umarbeiten, Bekanntgeben, Archivieren oder Vernichten von Daten». «Personendaten» werden definiert als «alle Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen», «besonders schützenswerte Personendaten» sind Daten über «die religiösen, weltanschaulichen, politischen oder gewerkschaftlichen Ansichten oder Tätigkeiten, die Gesundheit, die Intimsphäre oder die Rassenzugehörigkeit, Massnahmen der sozialen Hilfe, administrative oder

³ Erläuternder Bericht der Staatspolitischen Kommission des Nationalrates, 14. Februar 2020 (Fussnote 1), S. 5.

⁴ Bundesgesetz über den Datenschutz (DSG, SR 235.1).

strafrechtliche Verfolgungen und Sanktionen» und «Persönlichkeitsprofile» sind eine «Zusammenstellung von Daten, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer natürlichen Person erlauben».⁵

3. Völkerrechtliche Vorgaben

UNHCR erkennt an, dass Staaten ein berechtigtes Interesse haben, die Identität von Personen auf ihrem Staatsgebiet festzustellen und Asylentscheidungen auf der Grundlage der umfassendsten und genauesten verfügbaren Informationen zu treffen. Dies kann einen Zugriff auf personenbezogene Daten rechtfertigen.⁶ Gleichzeitig erachtet UNHCR die vorgeschlagene Ermächtigung, Datenträger von Asylsuchenden zur Feststellung der Identität, Nationalität oder Reiseroute sicherstellen und auswerten zu können, in dieser Form als bedenklich. Die Auswertung von Datenträgern wirft wichtige menschenrechtliche Fragen, wie etwa im Zusammenhang mit dem Recht auf Privatsphäre, auf. Eine Auswertung muss daher im Einzelfall jedenfalls notwendig und verhältnismässig sein. UNHCR vermisst in diesem Zusammenhang wichtige Schutzvorkehrungen in der vorgeschlagenen gesetzlichen Ausgestaltung. Zudem ist es wichtig festzuhalten, dass auf Mobilgeräten gespeicherte elektronische Daten in der Regel eine Reihe persönlicher und sensibler Informationen enthalten, die grossteils für die Feststellung der genannten Zwecke keine Relevanz haben. Eine ungezielte und willkürliche Auslesung von Daten würde somit über das Ziel einer Identitäts-, Nationalitäts- oder Reiseroutenfeststellung hinausgehen. In diesem Zusammenhang ist auch zu beachten, dass verschiedene Datenträger, wie etwa Mobiltelefone, im Rahmen einer Flucht oft von verschiedenen Personen (inklusive Schleppern) verwendet werden, was eine Zuordnung der Daten zum jeweiligen Asylsuchenden erschweren und somit die Zuverlässigkeit der ausgewerteten Daten beeinträchtigen kann.⁷

Weiter ist auch erforderlich, vorzusehen wie vor einer ungerechtfertigten Beschlagnahme und Durchsuchung persönlicher elektronischer Geräte geschützt werden kann. Solche eingreifenden Massnahmen sollten auch nicht zu einem routinemässigen Bestandteil des Asylverfahrens werden, sondern nur dann genutzt werden, wenn sie für die Prüfung des Schutzantrags erforderlich sind.⁸

Die Beschlagnahme und Durchsuchung elektronischer Datenträger greifen in Grund- und

⁵ Zu den Definitionen, siehe Art. 3 lit. a, c, d und e DSGVO.

⁶ UN High Commissioner for Refugees (UNHCR), *UNHCR Preliminary Legal Observations on the Seizure and Search of Electronic Devices of Asylum-Seekers*, 4 August 2017, S. 1, verfügbar unter: <https://www.refworld.org/docid/59a5231b4.html> [zuletzt besucht am 21.05.2020].

⁷ UNHCR *Preliminary Legal Observations on the Seizure and Search of Electronic Devices of Asylum-Seekers*, 4 August 2017 (Fussnote 6), S. 1 und 2. Siehe auch UN High Commissioner for Refugees (UNHCR), *UNHCR-Analyse des Entwurfs für das Fremdenrechtsänderungsgesetz 2018*, 9. Mai 2018, verfügbar unter: <https://www.refworld.org/docid/5afae4a64.html> [zuletzt besucht am 02.06.2020].

⁸ UNHCR *Preliminary Legal Observations on the Seizure and Search of Electronic Devices of Asylum-Seekers*, 4 August 2017 (Fussnote 6), S. 1.

Menschenrechte ein. Hierzu gehören unter anderem, das Recht auf Menschenwürde⁹, das Recht auf Privat- und Familienleben¹⁰ und das Recht auf Besitz, Nutzung und Verfügung über sein rechtmässiges Eigentum^{11, 12}. Zudem können auch andere Rechte beeinträchtigt sein, die zunehmend über digitale Medien ausgeübt werden.¹³

Im Folgenden wird jedoch lediglich auf das in erster Linie betroffene Recht auf Privatsphäre¹⁴ Bezug genommen, welches auch den Schutz persönlicher Daten miteinschliesst.¹⁵

4. Kommentare zum Vorentwurf SPK-N

Das Hochkommissariat der Vereinten Nationen für Menschenrechte stellte klar, dass jegliches Erfassen von Kommunikationsdaten, einschliesslich des Speicherns und Sammelns einen Eingriff in das Recht auf Privatsphäre darstellen kann.¹⁶

Der Gesetzesvorentwurf ermöglicht den Behörden Zugang zu Daten, die sehr sensible, private und teilweise intimste Bereiche der Lebensgestaltung von Asylsuchenden betreffen

⁹ Vgl. *Universal Declaration of Human Rights, 10 December 1948, 217 A (III) (UDHR), Article 1*, verfügbar unter: <http://www.refworld.org/docid/3ae6b3712c.html>, *International Covenant on Civil and Political Rights (16 December 1966) 999 UNTS 171 (ICCPR), Article 10*, abrufbar unter: <http://www.refworld.org/docid/3ae6b3aa0.html> (in der Folge wird die in der Schweiz übliche Abkürzung "UNO-Pakt II" verwendet).

¹⁰ Vgl. *Art. 17 UNO-Pakt II und European Convention for the Protection of Human Rights and Fundamental Freedoms (EMRK), as amended by Protocols Nos. 11 and 14, 4 November 1950, ETS 5, Article 8*, <http://www.refworld.org/docid/3ae6b3b04.html>.

¹¹ Vgl. *Art. 12 UDHR, Art. 17 UNO-Pakt II*.

¹² Vgl. zum Ganzen *UNHCR Preliminary Legal Observations on the Seizure and Search of Electronic Devices of Asylum-Seekers, 4 August 2017 (Fussnote 6)*, S. 2.

¹³ Dazu gehört beispielsweise das Recht auf Meinungsfreiheit und freie Meinungsäusserung, das Recht, sich Informationen zu beschaffen, zu empfangen und weiterzugeben, das Recht, sich friedlich zu versammeln und zu Vereinigungen zusammenzuschliessen; siehe Bericht des Amtes des Hohen Kommissars der Vereinten Nationen für Menschenrechte zum Recht auf Privatheit im digitalen Zeitalter, *A/HRC/27/37*, 30. Juni 2014, S. 5f., abrufbar unter: <https://www.un.org/depts/german/menschenrechte/a-hrc-27-37.pdf> [zuletzt besucht am 21.05.2020].

¹⁴ Da in diesem Zusammenhang oft der Begriff «Recht auf Privatsphäre» benutzt wird, wird in der Folge dieser Begriff verwendet (vgl. Bericht des Amtes des Hohen Kommissars der Vereinten Nationen für Menschenrechte zum Recht auf Privatheit im digitalen Zeitalter, 30. Juni 2014 (Fussnote 13), S. 5f. Die folgende Analyse des Rechts auf Privatsphäre erfolgt auf der Grundlage von Art. 17 UNO-Pakt II. Angesichts des vergleichbaren Schutzbereichs von Art. 8 EMRK würde eine Analyse dieser Norm zum gleichen Ergebnis führen. Zum vergleichbaren Schutzbereich siehe Manfred Nowak, *U.N. Covenant on Civil and Political Rights: CCPR Commentary, 2005*, art 2, p. 385, para 16.

¹⁵ Bericht des Amtes des Hohen Kommissars der Vereinten Nationen für Menschenrechte zum Recht auf Privatheit im digitalen Zeitalter, 30. Juni 2014 (Fussnote 13), S. 7.

¹⁶ Bericht des Amtes des Hohen Kommissars der Vereinten Nationen für Menschenrechte zum Recht auf Privatheit im digitalen Zeitalter, 30. Juni 2014 (Fussnote 13), S. 7. Auch der Europäische Gerichtshof für Menschenrechte (EGMR) hat bestätigt, dass persönliche Daten ein wesentliches Element des Rechts auf Privatsphäre (Art. 8 EMRK) sind (vgl. Schweizerisches Kompetenzzentrum für Menschenrechte (SKMR), *Das Recht auf Privatsphäre im digitalen Zeitalter, Staatliche Schutzpflichten bei Aktivitäten von Unternehmen*, 22. September 2016, S. 25, abrufbar unter: https://www.skmr.ch/cms/upload/pdf/160922_SKMR-Studie_Privatsphaere.pdf [zuletzt besucht am 22.05.2020]).

und in ihrer Gesamtheit genaue Schlüsse auf das Privatleben sowie auf wesentliche Aspekte der Persönlichkeit erlauben. Die im Gesetzentwurf vorgesehenen Massnahmen stellen daher einen schwerwiegenden Eingriff in das Recht auf Privatsphäre dar.¹⁷

4.1 Rechtmässigkeit

Ein solcher Eingriff muss gesetzlich vorgesehen und genügend detailliert sein, um Vorhersehbarkeit und Rechtssicherheit zu schaffen.

Der Vorentwurf sieht hingegen vor, dass der Bundesrat erst auf Verordnungsebene festlegt, welche Daten erhoben werden dürfen, wie der Zugriff durch Mitarbeitende des SEM zu regeln ist sowie wie allfällige weitere Einzelheiten der Auswertung zu regeln sind. Zudem werden die in Frage kommenden Datenträger im Gesetz nicht abschliessend genannt, um laut Erläuterungen der SPK-N «künftigen technischen Entwicklungen Rechnung» tragen zu können.¹⁸

Es bestehen daher Bedenken, dass der Gesetzesvorschlag nicht die notwendige Vorhersehbarkeit und Rechtssicherheit schafft. UNHCR erachtet es für wichtig, dass im Gesetz selbst unter anderem definiert wird, welche Daten erhoben werden dürfen beziehungsweise welche Daten für den definierten Zweck erforderlich sind. Dies ist insbesondere wichtig, da Datenträger ein breites Spektrum an Daten enthalten können, welche Grossteils nicht für den vorgesehenen Zweck relevant und notwendig sind. Aus diesem Grund muss eine präzise Triage der relevanten Daten vorgenommen werden, auch um eine ausufernde und damit willkürliche Auslesung von Personendaten und um den Zugriff auf Daten von Drittpersonen auf verlässliche Weise zu verhindern. Zudem ist im Gesetz zu regeln, wie der Zugriff durch SEM Mitarbeitende erfolgen soll, welche Daten bearbeitet werden dürfen, wie und für wie lange sie angeordnet werden können, welche Verfahren auf die Nutzung und Speicherung der gesammelten Daten zur Anwendung kommen, welche Datenträger für wie lange eingezogen werden können und wie die Rückgabe geregelt ist.¹⁹

Informationsverpflichtung und Einzelfallprüfung

Schutzsuchende müssen zudem umfassend über den Zweck der Einforderung eines Datenträgers und über die Bearbeitung ihrer persönlichen Daten informiert werden, wie beispielsweise über den Zweck der Bearbeitung, wie die Daten genutzt werden und welches

¹⁷ Dies wird auch vom Staatssekretariat für Migration SEM so gesehen, vgl. *Der Bund, Handys von Asylsuchenden geprüft - und fündig geworden*, 9. August 2019, abrufbar unter: <https://www.derbund.ch/schweiz/standard/bund-kontrolliert-handys-von-asylsuchenden/story/29531805> [zuletzt besucht am 21.05.2020].

¹⁸ Vgl. nArt. 8a Abs. 5 AsylG sowie *Erläuternder Bericht der Staatspolitischen Kommission des Nationalrates*, 14. Februar 2020 (Fussnote 1), S. 5.

¹⁹ Vgl. dazu ausführlich UNHCR *Preliminary Legal Observations on the Seizure and Search of Electronic Devices of Asylum-Seekers*, 4 August 2017 (Fussnote 6), S. 3.

Verfahren dafür vorgesehen ist, wie die Speicherung erfolgt und wo eine Bearbeitung angefochten werden kann, damit sie auf dieser Grundlage eine freie und informierte Zustimmung zur genannten Massnahme abgeben können.²⁰

Der Vorentwurf sieht keine solche Informationspflicht vor. Eine freie und informierte Zustimmung der betroffenen Person zur geplanten Massnahme kann daher nicht erfolgen. UNHCR empfiehlt deshalb eine umfassende Informationsverpflichtung in das formelle Gesetz aufzunehmen.

Ohne Einwilligung ist solch eine eingreifende Massnahme wie sie im Vorentwurf vorgeschlagen wird, nur dann gerechtfertigt, wenn in einer sorgfältigen Einzelfallprüfung abgeklärt wird, ob die Aushändigung von elektronischen Datenträgern und die Bearbeitung personenbezogener Daten im jeweiligen Einzelfallkontext notwendig und verhältnismässig sind. Eine routinemässige Anordnung dieser Massnahmen würde diesem Erfordernis nicht entsprechen. Die Prüfung ist dabei von zuständigen Personen durchzuführen, die über das entsprechende Fachwissen verfügen.²¹

UNHCR empfiehlt daher, das Erfordernis der Durchführung einer Einzelfallprüfung zur Bestimmung der Notwendigkeit und Verhältnismässigkeit durch die kompetente Behörde in das Gesetz aufzunehmen.

Wirksame und unabhängige Aufsichtsgremien

Eine genügende Rechtsgrundlage bei Überwachungspraktiken erfordert wirksame und unabhängige Aufsichtsgremien, welche die Massnahmen genehmigen und deren völker- und verfassungsrechtliche Konformität sicherstellen.²²

Im Vorentwurf ist weder ein Aufsichtsgremium noch eine Genehmigungspflicht für die Einforderung von Datenträgern oder für die Bearbeitung von personenbezogenen Daten vorgesehen. Dagegen ist die Auswertung von Mobiltelefonaten im Strafverfahren sehr restriktiv geregelt und nur bei dringendem Tatverdacht auf schwere Delikte zulässig. Zudem unterliegt sie in der Regel der Genehmigung durch ein Gericht.²³

UNHCR empfiehlt daher, die Einforderung eines Datenträgers zwecks Bearbeitung von Personendaten einer Genehmigungspflicht zu unterstellen und dafür ein unabhängiges

²⁰ Vgl. dazu ausführlich UNHCR Preliminary Legal Observations on the Seizure and Search of Electronic Devices of Asylum-Seekers, 4 August 2017 (Fussnote 6), S. 2.

²¹ Vgl. dazu ausführlich UNHCR Preliminary Legal Observations on the Seizure and Search of Electronic Devices of Asylum-Seekers, 4 August 2017 (Fussnote 6), S. 2f.

²² UNHCR Preliminary Legal Observations on the Seizure and Search of Electronic Devices of Asylum-Seekers, 4 August 2017, (Fussnote 6), S. 3 und Bericht des Amtes des Hohen Kommissars der Vereinten Nationen für Menschenrechte zum Recht auf Privatheit im digitalen Zeitalter, 30. Juni 2014 (Fussnote 13), S. 13f, 18.

²³ Vgl. Art. 198 und Art. 241 Abs. 1 Schweizerische Strafprozessordnung (StPO, SR 312.0). Eine Durchsuchung elektronischer Datenträger kann zwar auch die Staatsanwaltschaft anordnen, der Durchsuchungsbefehl muss aber in jedem Fall schriftlich erfolgen. Eine systematische und präventive Durchsuchung ist ausgeschlossen (siehe BGer, Urteil 6B_998/2017 vom 20.04.2018, E. 2.1.1.).

Aufsichtsgremium einzusetzen. Dieses hätte die Aufgabe, die völker- und verfassungsrechtliche Konformität der Anwendung der Massnahmen im Einzelfall zu überprüfen und nur bei Erfüllung der Voraussetzungen der Notwendigkeit und Verhältnismässigkeit eine Genehmigung zu erteilen.

Recht auf wirksamen Rechtsschutz

Asylsuchende, deren Geräte beschlagnahmt und deren persönlichkeitsnahe Daten bearbeitet wurden, müssen Zugang zu einem wirksamen Rechtsbehelf haben, um die Rechtmässigkeit der Beschlagnahme und Bearbeitung anzufechten und die Rückgabe der eingezogenen Geräte sicherzustellen.²⁴ Damit dieser Rechtsschutz Wirksamkeit entfaltet, beinhaltet dieser eine umgehende, gründliche und unparteiliche Untersuchung der geltend gemachten Verletzungen.²⁵

Der Vorentwurf enthält keine Ausführungen zur richterlichen Überprüfung geltend gemachter Verletzungen. Es wird lediglich vorgesehen, dass alle ausgewerteten Personendaten im Asylossier abzulegen sind und die asylsuchende Person sich dazu äussern kann (vgl. nArt. 8a Abs. 6 AsylG). Es bleibt jedoch unklar, was dies bedeutet und wie Asylsuchende eine Richtigstellung, Löschung usw. verlangen können.

Der Logik des Asylverfahrens zufolge müssten daher solche Einwände zusammen mit einer Verfügung des SEM vor dem Bundesverwaltungsgericht geltend gemacht werden. Damit ist jedoch eine «umgehende» Untersuchung unter Umständen nicht gewährleistet, da die Anordnung der Einforderung beziehungsweise Bearbeitung von Personendaten und eine erstinstanzliche Verfügung des SEM zeitlich auseinanderfallen können.

UNHCR empfiehlt deshalb, die umgehende Überprüfbarkeit erfolgter Einforderung eines Datenträgers und der Bearbeitung von Personendaten entweder im Sinne einer selbständig anfechtbaren Zwischenverfügung vor dem Bundesverwaltungsgericht im formellen Gesetz zu verankern. Alternativ bestünde die Möglichkeit, die Genehmigung des Aufsichtsgremiums als anfechtbare Entscheidung auszugestalten.

4.2 Notwendigkeit und Verhältnismässigkeit

Die Massnahmen müssen zur Erreichung eines legitimen Ziels notwendig und in Bezug auf das Ziel, der Feststellung der Identität, Nationalität und Reisewegs, tauglich und verhältnismässig sein sowie den mildesten Eingriff darstellen.

²⁴ UNHCR Preliminary Legal Observations on the Seizure and Search of Electronic Devices of Asylum-Seekers, 4 August 2017 (Fussnote 6), S. 3.

²⁵ Bericht des Amtes des Hohen Kommissars der Vereinten Nationen für Menschenrechte zum Recht auf Privatheit im digitalen Zeitalter, 30. Juni 2014 (Fussnote 13), S. 14.

Zwecktauglichkeit und Verhältnismässigkeit

Es ist zu bedenken, dass Mobiltelefone bei einer Flucht über einen langen Zeitraum manchmal von mehreren Personen, inklusive von Schleppern, verwendet werden. Dies kann eine Zuordnung der Mobiltelefonaten oder der Daten anderer elektronischer Datenträger wie SIM-Karten zu den entsprechenden Asylsuchenden erschweren und damit die Zuverlässigkeit der bearbeiteten Daten beeinträchtigen. Es kommt zwar vor, dass Asylsuchende ihre Identität verheimlichen. Andererseits vermeiden Asylsuchende es oft, ihre korrekten Namen auf sozialen Medienplattformen zu verwenden, auch um sich der Überwachung und möglichen Verfolgung oder einer möglichen Schädigung ihrer Familien im Herkunftsland zu entziehen. Ferner können digitale und elektronische Beweismittel in bestimmten Fällen nur eine begrenzte Zuverlässigkeit oder Genauigkeit aufweisen oder leicht verändert werden. Der Beweiswert elektronischer Datenträger, sollten sie zum Einsatz kommen, ist daher mit grosser Sorgfalt zu prüfen.²⁶

Der Vorentwurf sieht auch die Bearbeitungsmöglichkeit sehr privater, sensibler Daten vor. Dies wirft die Frage auf, ob die Bearbeitungsmöglichkeit solcher Daten nicht bereits den Kerngehalt des Rechts auf Privatsphäre berührt und somit das Recht für die betroffenen Asylsuchenden seinen Wesensgehalt verliert.²⁷ Zudem befinden sich auf den im Vorentwurf genannten Datenträgern (nArt. 8a Abs. 2 AsylG) eine Vielzahl von Daten, welche nicht dem Zweck dienen.

UNHCR ist besorgt, dass die vorgesehene Gesetzesänderung nicht genügend zweckgebunden und verhältnismässig ist und daher die Gefahr einer ungezielten und willkürlichen Einforderung, Auslesung und Bearbeitung von Daten entstehen kann.²⁸ Daher wird nahegelegt, den Vorentwurf auf diese Aspekte hin sorgsam zu überprüfen.

Evaluationen einer solchen Datennutzung in Deutschland haben zudem gezeigt, dass der Nutzen im Verhältnis zum hohen Aufwand solcher Datenauswertungen eher gering war.²⁹ Auch die in den Bundesasylzentren Chiasso und Vallorbe durchgeführten Pilotprojekte, auf

²⁶ UNHCR Preliminary Legal Observations on the Seizure and Search of Electronic Devices of Asylum-Seekers, 4 August 2017 (Fussnote 6), S. 2.

²⁷ Bericht des Amtes des Hohen Kommissars der Vereinten Nationen für Menschenrechte zum Recht auf Privatsphäre im digitalen Zeitalter, 30. Juni 2014 (Fussnote 13), S. 9.

²⁸ Vgl. dazu ausführlich UNHCR Preliminary Legal Observations on the Seizure and Search of Electronic Devices of Asylum-Seekers, 4 August 2017 (Fussnote 6), S. 3.

²⁹ Vgl. hierzu die Diskussion in Deutschland: Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Ulla Jelpke, Dr. André Hahn, Gökyay Akbulut, weiterer Abgeordneter und der Fraktion DIE LINKE. – Drucksache 19/5697, 19. Dezember 2018, S. 1f., abrufbar unter: <http://dipbt.bundestag.de/doc/btd/19/056/1905697.pdf>. Demnach wurden von Januar bis Juli 2018 knapp 7'000 Datenträger von Asylsuchenden ab 14 Jahren ohne Pass ausgelesen. In rund 2'000 Fällen wurden die ausgelesenen Daten auch ausgewertet. In 64 Prozent der Fälle gab es keine verwertbaren Ergebnisse, in 34 Prozent konnten die Angaben der Betroffenen bestätigt werden, und nur in zwei Prozent der Fälle wurden sie widerlegt. Trotz der Zweifel an der Verhältnismässigkeit der Massnahme will die Bundesregierung an der umstrittenen Handyauswertung festhalten (vgl. Bundestagsdrucksache 19/4961, S. 31ff).

welche der erläuternde Bericht der SPK-N³⁰ Bezug nimmt, in denen Asylsuchende auf freiwilliger Basis mobile Datenträger einreichen konnten, wiesen wenige nützliche Hinweise auf die Identität und Herkunft auf. Der Nutzen dieser Massnahme wurde deshalb bezweifelt.³¹

UNHCR unterstützt daher den Vorschlag der SPK-N, die Wirksamkeit der Einforderung von Datenträgern beziehungsweise die Bearbeitung von Personendaten von Asylsuchenden zwei Jahre nach einem allfälligen Inkrafttreten der Vorlage in einem Evaluationsbericht³² zu überprüfen. Wichtig wird dabei sein, quantitative Aussagen über die Anzahl Fälle machen zu können, in welchen zweckrelevante Hinweise gefunden werden konnten; zu belegen, welchen Daten zweckrelevante Hinweise lieferten; sowie das Verhältnis von Aufwand (personell und finanziell) und Ertrag aufzuzeigen. Weiter empfiehlt sich, die Auswertung nach dem jeweiligen Zweck (Feststellung der Identität, Nationalität und Reisewegs) zu unterscheiden, um so präzisere Rückschlüsse ziehen zu können.

Einzug und Bearbeitung als *ultima ratio*

Damit der Einzelne vor ungerechtfertigter Beschlagnahme und Durchsuchung elektronischer Geräte geschützt ist, braucht es die dafür notwendigen rechtlichen Schutzvorkehrungen, deren Standards weder eingeschränkt noch verweigert werden dürfen.³³ Solche Schutzvorkehrungen sehen vor, dass wenn weniger einschneidende Massnahmen oder Techniken zur Verfügung stehen, um den Zweck zu erfüllen, diese stattdessen angewendet werden sollten.³⁴

Der Vorentwurf sieht vor, dass dem SEM elektronische Datenträger auszuhändigen sind, wenn die Identität, die Nationalität oder der Reiseweg weder gestützt auf Identitätspapiere noch auf andere zumutbare Weise festgestellt werden können. Zu diesem Zweck soll laut erläuterndem Bericht den Asylsuchenden zuerst die Gelegenheit eingeräumt werden, von sich aus Angaben zur Nationalität, zur Identität oder zum Reiseweg zu machen.³⁵ Unter einer Feststellung «auf andere zumutbare Weise» versteht die SPK-N Massnahmen, welche im Vergleich zur elektronischen Datenauswertung mit geringerem Aufwand möglich sind. Dazu werden Angaben der Person selbst gerechnet oder auch andere Dokumente,

³⁰ Erläuternder Bericht der Staatspolitischen Kommission des Nationalrates, 14. Februar 2020 (Fussnote 1), S. 5.

³¹ Swissinfo.ch, SEM-Pilotprojekt wertet Handy- und Laptopdaten von Flüchtlingen aus, 10. August 2019, abrufbar unter: <https://www.swissinfo.ch/ger/alle-news-in-kuerze/sem-pilotprojekt-wertet-handy--und-laptopdaten-von-fluechtlingen-aus/45152994> [zuletzt besucht am 21.05.2020].

³² Erläuternder Bericht der Staatspolitischen Kommission des Nationalrates, 14. Februar 2020 (Fussnote 1), S. 6.

³³ UNHCR Preliminary Legal Observations on the Seizure and Search of Electronic Devices of Asylum-Seekers, 4 August 2017 (Fussnote 6), S. 1.

³⁴ UNHCR Preliminary Legal Observations on the Seizure and Search of Electronic Devices of Asylum-Seekers, 4 August 2017 (Fussnote 6), S. 3.

³⁵ Erläuternder Bericht der Staatspolitischen Kommission des Nationalrates, 14. Februar 2020 (Fussnote 1), S. 6.

die eindeutige Rückschlüsse auf die Identität zulassen. Ein Lingua-Gutachten wird jedoch in Bezug auf eine Auswertung elektronischer Daten nicht bevorzugt, da ein solches Verfahren mit einem grossen zeitlichen und organisatorischen Aufwand verbunden sei.³⁶

UNHCR teilt die Ansicht, dass die Angaben der Person selbst einer Bearbeitung elektronischer Daten vorgehen soll, da dies eine deutlich mildere Massnahme darstellt. Dies bedingt jedoch, dass zuerst eine Anhörung (oder Gewährung des rechtlichen Gehörs) durchgeführt wird, denn erst dort besteht die Möglichkeit ausführliche Informationen zu Identität, Nationalität und Reiseweg geben zu können. Es ist deshalb aber nicht ersichtlich, weshalb die SPK-N eine Bearbeitung von Personendaten grundsätzlich bereits in der Vorbereitungsphase vorsehen will (vgl. auch nArt. 8a Abs. 4 AsylG), welche zeitlich jedoch vor der Anhörung endet.

UNHCR empfiehlt deshalb, den Anwendungsvorrang von Massnahmen mit geringerer Eingriffsintensität im Asylgesetz selbst zu verankern und festzulegen, dass diese zuerst ausgeschöpft werden müssen, bevor zur nächsten einschneidenderen Massnahme gegriffen werden darf. Der vorgesehene Zugriff auf elektronische Datenträger stellt daher die *ultima ratio* dar.

UNHCR empfiehlt ebenfalls, auf Gesetzesebene explizit und abschliessend die Daten aufzulisten, die vom SEM oder anderen Behörden als *ultima ratio* bearbeitet werden dürfen. Bei dieser Auflistung ist darauf zu achten, dass ausschliesslich Daten für den im Gesetz aufgeführten Zweck Feststellung der Identität, der Nationalität oder des Reisewegs aufgeführt werden und dass die Bearbeitung von Daten, die in den Kernbereich der Privatsphäre eingreifen könnten, ausgeschlossen werden.

5. Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter (EDÖB)

UNHCR erachtet es für sinnvoll, den Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) in die Ausarbeitung der Vorlage einzubeziehen. Dies würde erheblich dazu beitragen, datenschutzrechtliche Bedenken, welche die Vorlage aufwirft, detailliert zu analysieren und den Vorentwurf in Einklang mit datenschutzrechtlichen Garantien zu bringen. Zu denken ist dabei an verschiedene weitere Fragen, welche die Vorlage aus datenschutzrechtlichen Gründen aufwirft, wie die vorgesehene Zwischenspeicherung (nArt. 8a Abs. 3 AsylG), die Weiterleitung an andere Behörden (Sicherheitsbehörden gemäss Art. 22a BPG / Art. 20 Abs. 3 und 4 NDG; kantonale Behörden, nArt. 47 Abs. 3 AsylG), den Einbezug von Dritten für den Einzug von Datenträgern (Art. 26 Abs. 5 AsylG), wie auch die Frage der Involvierung von geschützten Daten von Drittpersonen.

³⁶ Erläuternder Bericht der Staatspolitischen Kommission des Nationalrates, 14. Februar 2020 (Fussnote 1), S. 6.

6. Zusammenfassung der Empfehlungen

Auch wenn die genannten Ziele der Vorlage legitime Interessen zum Ausdruck bringen, erachtet UNHCR es für sinnvoll, den Vorentwurf im laufenden Verfahren einer umfassenden Prüfung der völker- und verfassungsrechtlichen Konformität zu unterziehen. Um diese Aufgabe zu unterstützen, sind die Empfehlungen von UNHCR untenstehend zusammengefasst.

UNHCR empfiehlt für das laufende Gesetzgebungsverfahren:

- **Umfassende Prüfung der völker- und verfassungsrechtlichen Konformität des Vorentwurfes;**
- **Einbezug des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) in die Ausarbeitung der Vorlage.**

UNHCR empfiehlt in Hinblick auf den Vorentwurf die Rahmenbedingungen der Einforderung von Datenträgern und die Bearbeitung von Personendaten detailliert, umfassend und klar in einem Gesetz im formellen Sinn zu verankern. Diese beinhalten:

- **Verankerung der Erforderlichkeit einer Einzelfallprüfung zur Bestimmung der Notwendigkeit und Verhältnismässigkeit durch die dafür kompetente Behörde;**
- **Verankerung des Anwendungsvorrangs von Massnahmen mit geringerer Eingriffsintensität in Art. 8 Abs. 1 AsylG sowie des *ultima ratio*-Charakters der vorgesehenen Massnahmen;**
- **Abschliessende Regelung, welche elektronischen Datenträger eingezo-gen werden dürfen sowie eine klare Regelung der Dauer und der Rückgabe elektronischer Datenträger;**
- **Klare Triage und Definition, welche Personendaten für den erforderli-chen Zweck erhoben werden dürfen unter Ausschluss nicht zwecknot-wendiger Daten, sowie Daten von Drittpersonen;**
- **Klare Regelung des Zugriffs auf elektronische Datenträger und die Be-arbeitung von Personendaten durch SEM Mitarbeitende; Ermächtigung ausschliesslich für dafür geschulte Mitarbeitende des SEM;**

- **Klare Regelung der Abläufe der Datenerhebung, Zwischenspeicherung und Auswertung;**
- **Umfassende Informationsverpflichtung über die Einforderung von Datenträgern und die Bearbeitung von Personendaten;**
- **Genehmigungspflicht für die Einforderung von Datenträgern und die Bearbeitung von Personendaten durch ein unabhängiges Aufsichtsgremium in der Einzelfallanwendung;**
- **Richterliche oder zumindest administrative Überprüfbarkeit erfolgter Einforderung von Datenträgern und die Datenbearbeitung als selbständigen Anfechtungsgrund;**
- **Verankerung der Pflicht zur Evaluation der Geeignetheit der Einziehung von Datenträgern bzw. Bearbeitung von Personendaten zwei Jahre nach einem allfälligen Inkrafttreten der Vorlage und Aufnahme der relevanten Parameter.**

UNHCR Büro für die Schweiz und Liechtenstein

Juni 2020