

HERAUSFORDERUNGEN DES DATENSCHUTZES IN DER POLITIK GEGEN MENSCHENHANDEL

Ein Praxisleitfaden

dataACT

data protection in anti-trafficking action

Herausforderungen des Datenschutzes in der Politik gegen Menschenhandel

Ein Praxisleitfaden

Herausgeber

Bundesweiter Koordinierungskreis gegen Menschenhandel e.V. (KOK e.V.)

Autorinnen

Pia Roth, Dr. Bärbel Heide Uhl, Marjan Wijers, Wiesje Zikkenheiner.
Die Autorinnen danken Marieke van Doorninck, Ulrike Gatzke und
Tabea Richter für ihre wertvollen Kommentare und Anmerkungen.

Design und Satz

Kathrin Windhorst, Tim Haberstroh

Druck

OKTOBERDRUCK AG, Berlin

Diese Publikation wurde durch die finanzielle
Unterstützung der OAK Stiftung ermöglicht.

© KOK e.V. 2015

Alle Rechte vorbehalten.

Bezugsadresse

info@kok-buero.de

KOK e.V.
Kurfürstenstraße 33
10785 Berlin

www.kok-gegen-menschenhandel.de
www.dataact-project.org

Das Projekt dataACT ist eine Kooperation des KOK e.V und La Strada International.
Diese Veröffentlichung stellt keine Meinungsäußerung des KOK e.V. dar.
Für inhaltliche Aussagen tragen die Autorinnen die Verantwortung.
Jegliche Reproduktion nur mit Genehmigung des KOK e.V.

INHALTSVERZEICHNIS

Vorwort: Menschenhandel im Spannungsfeld von Daten und Wissen, von Dr. Claudia Aradau	7
1. Einleitung	17
2. Zentrale Instrumente des Datenschutzes	20
3. Das Konzept „sensibler Daten“ und die verpflichtende Registrierung von Sexarbeiter*innen als Mittel zur Bekämpfung des Menschenhandels	55
4. Spezifische Datenschutzvorkehrungen in Rechtsinstrumenten zur Bekämpfung des Menschenhandels	62
5. Herausforderungen an den Datenschutz in den Richtlinien zur Bekämpfung des Menschenhandels	66
5.1 Nationale Berichterstattungsstellen (NREM) und andere Instrumente zur Datenerhebung	67
5.2 Identifizierung der vom Menschenhandel betroffenen Personen und Zugang zu Unterstützungsstrukturen	82
5.3 Datenschutz und spezialisierte Fachberatungsstellen für Betroffene von Menschenhandel	90
Anhang I: Die Rechte des Datensubjekts	98
Anhang II: datACT-Standards	100
Literaturangaben zum Vorwort	109
Ausgewählte Literaturangaben	111

GLOSSAR/ABKÜRZUNGSVERZEICHNIS

AECT	Alliance Expert Coordination Teams
AWF	Analytic Work File
CEDAW	Convention on the Elimination of all Forms of Discrimination against Women
CoE	Council of Europe
CTM	Counter-Trafficking Module
DCIM	Data Collection and Information Management
DSB	Nationale Datenschutzbehörde
ECHR	European Court of Human Rights
EDPS	European Data Protection Supervisor / europäische Datenschutzbeauftragte
EDV	Elektronische Datenverarbeitung
EFTA/EEA	Europäische Freihandelsassoziation / Europäische Ökonomische Vereinigung
EG	Europäische Gemeinschaft
EGMR	Europäischer Gerichtshof für Menschenrechte
EU	Europäische Union
EuGH	Europäischer Gerichtshof
Eurostat	Statistische Amt der Europäischen Union
Frontex	Europäische Agentur für die operative Zusammenarbeit an den Außengrenzen der Mitgliedstaaten der Europäischen Union

ICMPD	International Centre for Policy Development
IKT	Informations- und Kommunikationstechnik
ILO	International Labour Organization
IOM	International Migration Organization
MONTRASEC	Monitoring Trafficking in human beings and Sexual Exploitation of Children
NREM	National Rapporteurs on Trafficking in persons and Equivalent Mechanisms
NRO	Nichtregierungsorganisation
OSZE	Organisation für Sicherheit und Zusammenarbeit in Europa
PIA	Privacy Impact Assessment
TRM	Transnational Referral Mechanisms
UN	United Nations
UN.GIFT	United Nations Global Initiative to Fight Human Trafficking
UNODC	United Nations Office on Drugs and Crime
Wbp	Niederländisch: Wet bescherming persoonsgegevens – niederländische Umsetzung der Datenschutzrichtlinie

VORWORT

Der Menschenhandel im Spannungsfeld von Daten und Wissen

Dr. Claudia Aradau¹

Es ist mittlerweile allgemein anerkannt, dass der Komplexität des Phänomens Menschenhandel mit „differenzierten Maßnahmen“ bzw. „holistischen Ansätzen“ zu begegnen ist – wie es in der Fachliteratur heißt. Das beschränkte oder gar fehlende Wissen über den Menschenhandel verhindert wirkungsvollere Maßnahmen zu seiner Bekämpfung. „Mangelndes Wissen“ über das Phänomen wird häufig als das größte Hindernis für einen besseren staatlichen Umgang (Governance) mit dem Problem gesehen. Expert*innen sind sich mittlerweile darüber einig, dass die „Verbesserung der Datenlage“ einer der notwendigen Schritte zur Entwicklung wirkungsvollerer Strategien gegen den Menschenhandel darstellt (Laczko 2002, 2007). Es heißt, die Daten zum Menschenhandel seien nicht ausreichend, nicht zuverlässig, nicht vergleichbar und beschränkt (Ogrodnik 2010). Antonio Maria Costa, der ehemalige Direktor der UNODC, bezeichnet dies gar als „Wissenskrise“, deren Auswirkungen auf Maßnahmen zur Bekämpfung des Menschenhandels er folgendermaßen beschreibt:

- » Nur ein detailliertes Verständnis der verschiedenen Ebenen des Problems wird es uns erlauben, [...] tatsächlich etwas dagegen zu unternehmen. Bisher haben wir noch kein ausreichendes Wissen gewonnen. Somit waren bisherige Initiativen dem Problem weder gewachsen noch breit genug aufgestellt. (UNODC 2009b)

Von dieser Warte aus betrachtet scheitern die Bekämpfung des Menschenhandels, der Opferschutz und die Präventionsarbeit am systembedingten Mangel an Wissen. Letztlich liegt dem ein einfacher Gedanke zu Grunde:

1 Dr. Claudia Aradau, Dozentin für Internationale Politik, King's College, London, GB, ist eine international anerkannte Forscherin auf dem Gebiet der Datenpolitik. Das Vorwort stellt ihre Eröffnungsrede auf der internationalen datACT-Konferenz „Datenschutz und das Recht auf Datenschutz und informationelle Selbstbestimmung für marginalisierte Gruppen: eine neue Herausforderung in der Politik zur Bekämpfung des Menschenhandels“ dar, die vom 25. bis 27. September 2013 in Berlin stattfand.

Das Problem des Menschenhandels lässt sich durch eine Verbesserung der Datenlage lösen. Allerdings werden die dem postulierten Mangel an Daten zugrundeliegenden Annahmen und die unterschiedlichen Interpretationen dieses Mangels nirgends diskutiert. Stattdessen sollen mehr Daten umgehend zu effizienteren Maßnahmen und besseren Mechanismen für Opferschutz und Prävention führen.

Bei diesen Debatten lag der Fokus stets auf Maßnahmen, ohne dabei zu hinterfragen, ob das Problem der Datengewinnung als solches auf solidem Fundament steht. Wie jede*r Sozialwissenschaftler*in bestätigen kann, können falsche Fragen jedoch niemals zu richtigen Antworten führen, egal wie viel Mühe auch in die Formulierung der Antworten fließen mag. Hier soll es nun um die Frage von Daten in den staatlichen Strategien zur Bekämpfung des Menschenhandels gehen, und insbesondere um eine Betrachtung derselben im breiteren Kontext des konstatierten Mangels an Wissen. Was bedeutet es, zu sagen, dass es einen Mangel an Wissen über den Menschenhandel gibt? Meiner Meinung nach bestehen zunächst einmal drei mögliche Interpretationsansätze zum Verständnis dieses Mangels: Ignoranz, Geheimhaltung und Unsicherheit. Jeder dieser Ansätze wirkt sich unterschiedlich darauf aus, wie Daten gewonnen und wie und zu welchem Zweck Daten weiterverarbeitet werden. Für jeden dieser Fälle schlage ich einen eigenen Ansatz zum Umgang mit dem Mangel an Wissen über den Menschenhandel vor.

Ignoranz: Fortbildung und Sensibilisierung

Mangelndes Wissen über den Menschenhandel wurde zunächst als ein Problem von Ignoranz dargestellt. Ignoranz hat viele Gesichter: das Unwissen der Betroffenen von Menschenhandel über legale Möglichkeiten zur Migration, über Rechte und Schutzmöglichkeiten oder die Ignoranz der Behörden gegenüber dem Phänomen des Menschenhandels. Ein Handbuch für Journalist*innen in Serbien, verfasst von einer lokalen NRO, die zum Thema Menschenhandel arbeitet und von der OSZE unterstützt wird, fasst Ausmaß und Formen der Ignoranz zusammen:

- » Unter anderem ist es der Mangel an Wissen, insbesondere junger Frauen, über ihre Möglichkeiten zur Migration nach Westeuropa, der den Menschenhändlern in die Hände spielt. Diese Frauen verfügen entweder über ein nur geringes oder gar kein Wissen über die tatsächlichen Lebensverhältnisse und Arbeitsmöglichkeiten in der EU. Ihre Rechte kennen sie nicht und sie wissen auch nicht, ob und wie sie legal eine Arbeitserlaubnis bekommen können. Weder ist ihnen klar, dass ein (Schengen-) Touristenvisum nicht zur Arbeit berechtigt, noch sind sie sich im Mindesten der Gefahren bewusst, ‚schwarz‘ zu arbeiten. (ASTRA Anti-Trafficking Action 2009, 14)

Solcherlei Umstände werden als die Haupthindernisse für die Selbstwahrnehmung der Betroffenen als Opfer von Menschenhandel und für effiziente Maßnahmen zur Bekämpfung desselben betrachtet. Weitere emotional begründete Faktoren, wie etwa die Angst vor den Menschenhändler*innen, das Misstrauen gegenüber den Behörden und die psychologische Abhängigkeit von den Menschenhändler*innen beruhen letztlich ebenfalls auf Ignoranz: Es ist die Unkenntnis darüber, dass die Menschenhändler*innen bestraft werden und die Behörden Schutz bieten können und dass sie sich als Betroffene von Menschenhandel in einer Situation der Ausbeutung befinden.

Das Problem der Ignoranz soll sodann mit Maßnahmen zur Sensibilisierung und der Entwicklung von Fortbildungsangeboten gelöst werden². Sensibilisierungskampagnen und umfassende Weiterbildungsangebote für Richter*innen, Polizist*innen, Grenzschützer*innen und weitere Personen wurden vorgeschlagen und umgesetzt³. Hierbei handelt es sich um eine umfassende Aufklärungskampagne zum Thema Menschenhandel, mit der der Ignoranz auf allen Ebenen begegnet werden soll und die deshalb – so die Annahme – nicht nur schützend, sondern auch auf die Zukunft gerichtet präventiv wirken soll. Die Schulung von Mitarbeiter*innen, damit sie die Betroffenen von Menschenhandel erkennen, soll für einen besseren Umgang mit dem Problem sorgen.

2 Ausführliche Diskussionen finden sich in Andrijasevic 2007 und Aradau 2004.

3 Siehe ICMPD 2002 und 2004, UNODC 2009a.

Die Fortbildungshandbücher sollen dabei auf den zur Verfügung stehenden Daten zum Menschenhandel basieren und die Expert*innen lehren, die „Zeichen“ von Menschenhandel in Fällen zu erkennen, wo entweder potenziellen Betroffenen die Gefahr, in der sie schweben, oder aber tatsächlichen Betroffenen ihre eigentliche Situation nicht bewusst ist.

Bisher hat es allerdings nur sehr wenige Diskussionen über das Konzept der Ignoranz an sich gegeben, auf dem die Aufklärungspraxis zum Thema Menschenhandel beruht. Expert*innen, dies setzen die bisherigen Debatten voraus, kennen den Unterschied zwischen Wissen und Ignoranz. Sie wissen somit auch, wer in Bezug auf welche Fragen ignorant ist. Aus mindestens zweierlei Gründen sind derartige Annahmen schwierig. Zum einen verweigert ein solcher Ansatz Frauen die Anerkennung als erkenntnistheoretische Akteure. Wissen, das die Betroffenen von Menschenhandel über ihre Situation vielleicht haben, wird als „Ignoranz“ disqualifiziert. Möglicherweise nützliche Daten gehen dadurch automatisch verloren, außer sie passen zu bereits etabliertem Wissen. Zum anderen impliziert dieser Ansatz, dass sich Ignoranz durch das ausschließlich einigen Expert*innen zur Verfügung stehende Wissen bekämpfen lässt. Ignoranz ist somit ein Mangel, eine Wissenslücke, die sich durch die Anhäufung von Wissen bekämpfen lässt, und kein Produkt der sozialen Interaktionen zwischen verschiedenen Expertengruppen oder zwischen Expert*innen und den „Opfern des Menschenhandels“. Die Feministin Nancy Tuana prägte für die produktive Funktion und konstruierte Form der Ignoranz den Begriff „Epistemologie der Ignoranz“⁴. Ignoranz und Wissen koexistieren immer und jede Produktion von Wissen bringt auch Ignoranz hervor. Hier geht es nicht um wahr oder falsch, sondern darum, wie Wissen entwertet bzw. als illegitim dargestellt wird. Strategien zur Bekämpfung des Menschenhandels erfordern daher, größere Sorgfalt walten zu lassen und Annahmen von „mangelndem Wissen“ und Ignoranz in Frage zu stellen.

Erstens müssten wir Wissen als situativ begründet und nicht als Mangel begreifen. Zu behaupten, bestimmte Personen seien ignorant, lässt gewisse Stimmen als weniger wichtig oder gar illegitim erscheinen. Statt von einem

4 Sullivan und Tuana 2007.

Mangel an Wissen auszugehen, wie wäre es, das Wissen der Betroffenen als Wissen anstatt als Nicht-Wissen/Ignoranz zu betrachten? Zweitens müssten wir verstehen, wie sich die konstatierte Ignoranz zu ganz bestimmten Zwecken strategisch nutzen lässt. Was bedeutet es, wenn davon gesprochen wird, dass Expert*innen den Menschenhandel aus einem Mangel an Wissen heraus nicht als solchen erkennen? Wie wäre es, wenn wir ihr situatives Wissen als wichtig und gültig verstehen würden, anstatt es als Ignoranz abzutun? Zu guter Letzt gehen Fortbildungsmaßnahmen und Sensibilisierungskampagnen davon aus, dass Wissen das Handeln von Menschen beeinflusst. Jedoch ändern diese Kampagnen nichts an den materiellen Bedingungen, unter denen Menschen leben. Aber ohne ein Verständnis für die Handlungsbedingungen der Betroffenen werden Lernen und Schulungsmaßnahmen weiterhin ohne Effekt bleiben.

Geheimhaltung: Mechanismen der Überwachung und Identifikation

Eine zweite wichtige Form des Wissensmangels offenbart sich in der Repräsentation von Menschenhandel als Phänomen eines kriminellen Milieus. Ein Bericht von Amnesty International merkt an: „Als Geschäft läuft der Menschenhandel im Untergrund. Daher sind genaue Informationen über das Ausmaß in Großbritannien nur schwer zu bekommen“ (Amnesty International 2013). Weil er illegal ist, läuft der Menschenhandel im Dunkeln ab. Die Durchbrechung der Geheimhaltung wird somit zu einer neuen Strategie, die Maßnahmen gegen den Menschenhandel effektiver machen sollen. Gebraucht werden folglich Daten zu geheimen Organisationen, der Schattenwirtschaft und zu den Personen, die zu diesen Organisationen und der Schattenwirtschaft Beziehungen zu pflegen scheinen.

Dabei kommt es allerdings zu einer bedeutenden Verschiebung im Spannungsfeld von Geheimhaltung einerseits und Schutz der Privatsphäre andererseits, die sich wiederum auf alle vom Menschenhandel Betroffenen auswirkt. Traditionell wurde das Recht auf Privatsphäre unter anderem als das Recht verstanden, sich zurückziehen, sich isolieren und Dinge im Dun-

keln belassen zu können. Wie Warren und Laslett in ihrem Vergleich von Geheimhaltung und dem Schutz der Privatsphäre anmerken, ist „Geheimhaltung, im Gegensatz zur Privatsphäre, die einfach ein Rückzug aus dem öffentlichen Raum ist, ein sich über diese Ordnung hinwegsetzendes oder gegen diese Ordnung gerichtetes Agieren“ (1977). Während der Schutz der Privatsphäre als legitim erscheint, gilt dies – auf Personen oder bestimmte nichtstaatliche Gruppen bezogen – nicht für die Geheimhaltung. Wird die Privatsphäre als der Raum verstanden, in dem nur engste Vertraute Zugang zum persönlichen Wissen einer Person haben, würde der Zwang zur Wissensmehrung, sobald Geheimhaltung prinzipiell problematisiert wird, ein Mandat zur Sammlung geheimer Privatinformationen etablieren:

- » Aus der Geheimhaltung, die alles umhüllt, das tiefgreifend und bedeutsam ist, erwächst das typische Missverständnis, wonach alles Mysteriöse auch wichtig und von wesentlicher Bedeutung ist. Im Angesicht des Unbekannten arbeiten der menschliche Hang zur Idealisierung und die menschliche Furchtsamkeit gemeinsam in Richtung des gleichen Ziels: der Intensivierung des Unbekannten durch die Fantasie. Dem Unbekannten wird eine Aufmerksamkeit zuteil, die der gewöhnlichen Realität in dieser Intensität normalerweise nicht zuteil wird. (Wolff 1950, 333)

Implizit verlangt ein solcher Ansatz nach Überwachung, denn sie allein gewährt Zugang zu dieser geheimen Welt und ermöglicht die Identifizierung der in ihr operierenden Personen. Für den Menschenhandel bedeutet dies: Die Offenlegung des Geheimen ist gewichtiger als der Schutz der Privatsphäre.

Indem sie das Nicht-Wissen über den Menschenhandel einfach als die nicht legitimen Geheimnisse krimineller Organisationen einordnen, verringern solche Strategien zur Bekämpfung des Menschenhandels den Spielraum für Sorgen über den Schutz der Privatsphäre. Daher sollte Geheimhaltung als Konzept sehr viel sorgfältiger analysiert werden, als dies bisherige Stellungnahmen zum organisierten Verbrechen tun. Ein Punkt, den wir bei diesen Debatten bedenken müssen, ist, dass Geheimhaltung lange eine Strategie der gesellschaftlich Marginalisierten und

somit eine Möglichkeit war, sich dem Zugriff der Mächtigen zu entziehen. Wie der Soziologe Georg Simmel zeigt, kann Geheimhaltung eine Form des Selbstschutzes sein: „Allgemein gesagt, entstehen Geheimgesellschaften immer als Antwort auf Despotismus und Polizeiherrschaft. Sie bieten Schutz und sind dabei zugleich Verteidigung gegen und Angriff auf den gewaltförmigen Druck zentralisierter Macht“ (Simmel 1906, 472). Mehr noch, Simmel warnt vor dem Trugschluss, alles Geheime als entweder wichtig oder nicht legitim anzusehen. Geheimhaltung ist sowohl allgemeiner Bestandteil zwischenmenschlicher Interaktionen als auch eine besondere Strategie des Selbstschutzes marginalisierter Gruppen. Wie Ignoranz auch wird Geheimhaltung je nach Akteuren oder Gruppen als illegitim konstruiert. Die Legitimität von Geheimhaltung wird dann akzeptiert, wenn sie in der Form des Vorrechts von Expert*innen im Kampf gegen den Menschenhandel auftritt. Organisationen wie Frontex⁵ argumentieren beispielsweise, dass „aufgrund der sensiblen Natur der Risikoprofile“ der von Menschenhandel Betroffenen, diese nur den Polizeibehörden zur Verfügung stehen sollten (2011). Die Produktion von Wissen bringt in diesem Fall auch Nicht-Wissen hervor, da die Geheimhaltung bestimmte Akteure auf Kosten anderer als Wissende legitimiert. Aber wer darf Geheimnisse haben? Solange Wissensbeziehungen von Vertrauensbeziehungen untermauert sind, wird Geheimhaltung nicht hinterfragt. Anders gesagt, macht fehlendes Vertrauen Geheimhaltung inakzeptabel. Daher ist die Frage von mangelndem Wissen und Geheimhaltung auch eine Frage über die Herstellung und den Entzug von Vertrauen.

Unsicherheit: Datensammlung als Strategie

Der dritte Interpretationsansatz für mangelndes Wissen ist das Konzept Unsicherheit. Der Menschenhandel wird als sich schnell wandelndes Phänomen begriffen. Die Sammlung und Weiterverarbeitung von Daten wird daher als Möglichkeit zum besseren Verständnis zukünftiger Entwicklungen gesehen.

⁵ Europäische Agentur für die operative Zusammenarbeit an den Außengrenzen der Mitgliedstaaten der Europäischen Union (Frontex; European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union).

Das Datensammeln ist in diesem Fall kein Heilmittel für eine vermutete Ignoranz der Expert*innen, sondern vielmehr ein Mittel zum Umgang mit der unbestimmten Natur des Phänomens. Der Opferschutz und die Verhinderung des Menschenhandels setzt eine gewisse Prognosefähigkeit auf Seiten der Expert*innen voraus: Wie agieren die Menschenhändler*innen wohl und wie reagieren die Betroffenen darauf usw.? Angesichts der Unwägbarkeiten im Bereich des Menschenhandels schlägt die EU-Kommission daher die „Strategie der EU zur Beseitigung des Menschenhandels 2012–2016“ vor und schafft so ein System zur Datensammlung:

- » Bei allen Formen des Menschenhandels verändern sich die Tendenzen, Muster und Arbeitsmethoden der Menschenhändler, die sich auf das wechselnde Angebot und die sich wandelnde Nachfrage einstellen. Oft sind verschiedene Formen der Ausbeutung eng miteinander verbunden und gehen ineinander über, was die Identifizierung der genauen Form der Ausbeutung des jeweiligen Opfers erschwert. Dadurch wird die Erkennung von Opfern noch schwieriger. Ein rasches Verstehen dieser Tendenzen sowie eine effiziente Reaktion hierauf sind unabdingbar. (EU-Kommission 2012)

Schwerpunktmäßig betrachtet die EU den Menschenhandel als ein prioritäres Feld für die Sammlung von Daten und konzentriert sich auf die Entwicklung einer „Methodik und [...] Datenerhebungsmethoden im Hinblick auf die Erstellung vergleichbarer Statistiken“ (EU-Kommission 2012). Als Lösung für die konstatierte Wirkungslosigkeit der existierenden Richtlinien gegen den Menschenhandel erscheint die Erhebung von mehr und präziseren Daten. Es geht hier nicht nur um Ignoranz oder Geheimhaltung, sondern auch um Unsicherheit. Es herrscht Unklarheit darüber, welche neuen Methoden, neuen Routen, neuen Betroffenen und neuen Formen der Ausbeutung Menschenhändler*innen entwickeln könnten. Hier wirkt eine andere Präventionslogik: Gelungene Präventionsarbeit hängt dabei weder von der Bekämpfung von Ignoranz noch von der Offenlegung von geheim gehaltenem ab, sondern einzig von der Verringerung von Unsicherheit durch die Sammlung von Daten.

Über die Sammlung und Weiterverarbeitung dieser Daten findet sich nicht viel in den entsprechenden EU-Dokumenten. Ein Eurostat⁶-Bericht (2012) weist darauf hin, dass „Unsicherheit“ mittels statistischer Berechnungen zu einer „Risikoeinschätzung“ wird. Historisch betrachtet haben Risiko-Wahrscheinlichkeitsberechnungen, die Erstellung von Risikoprofilen und die Zuordnung von Risikofaktoren als Antworten auf Unsicherheit gedient. Mithilfe von individuell erhobenen Daten werden neue Kategorien und Profile entwickelt, ohne jedoch die inhärente Logik sichtbar zu machen. Aber weil diese Logik für sie nicht greifbar ist, können Individuen ihr auch nicht widersprechen.

Datenschutzbedenken wurden insbesondere in Bezug auf die Sammlung von Daten geäußert. Abschließend folgen daher ein paar Anmerkungen zum Datenschutz, der an sich ein wichtiges Recht ist, aber leider kein probates Mittel gegen die Probleme darstellt, die entstehen, wenn als Antwort auf Unsicherheit statistische Daten erhoben und Risikoprofile erstellt werden. Die Ersetzung des Individuums durch Risikokategorien führt dazu, dass der Datenschutz bei der Datensammlung nicht mehr anwendbar ist. Während die verschiedenen Datenkategorien für unser Verständnis des Menschenhandels hilfreich und im Sinne des Schutzes von Persönlichkeitsrechten weitestgehend unproblematisch erscheinen mögen, sind es nicht die Daten an sich, sondern ihre Aufbereitung und spätere Nutzung durch die verschiedenen Behörden, die problematisch sind. Wenn Sie Bürger* in eines der 10 Herkunftsländer sind, welche Auswirkungen hat das auf Ihre Möglichkeiten, sich frei zu bewegen, wenn Sie im Konsulat oder bei einer Grenzbehörde vorstellig werden? Antoinette Rouvroy und Yves Poulet weisen auf Folgendes hin:

- » [D]ie Sammlung großer Datenmengen und die intensive Nutzung von Daten erlauben den für die Verarbeitung Verantwortlichen, also Regierungsbehörden oder privaten Unternehmen, auf Basis der gesammelten und verarbeiteten personenbezogenen Daten Entscheidungen über Individuen zu fällen, ohne dass die Betroffenen die Möglichkeit haben, zu wissen, genau welche

6 Eurostat ist das Statistische Amt der Europäischen Union.

Daten, zu welchem Zweck und über welchen Zeitraum verarbeitet werden, und ohne ihnen eine Kontrolle über die Notwendigkeit dieser Vorgänge in Bezug auf die von der öffentlichen oder privaten Bürokratie verfolgten Zwecke zu gewähren. (Rouvroy und Poullet 2009, 68–69)

Wie mir scheint, stehen die Herausforderungen bei der Bekämpfung des Menschenhandels in Zusammenhang mit der Frage, wie wir verantwortlich wissen können. Es geht nicht darum, Wissen um jeden Preis zu fordern. Insbesondere muss gefragt werden, wie wir auf eine Weise wissen können, die weder die Freiheit noch die menschliche Würde untergräbt. Eine Möglichkeit wäre, von situativem Wissen auszugehen und die Art und Weise zu analysieren, wie dieses Wissen jeweils ignoriert oder unsicher werden kann. Zweitens müssten wir uns von der Vorstellung lösen, dass es so etwas wie „rohe“ Daten gibt, die uns helfen können zu verstehen, wie wir in Zukunft handeln sollten, um den Menschenhandel heute und morgen zu verhindern. Es gibt keine rohen Daten, genauso wenig wie es unschuldige Daten gibt. Darüber hinaus bieten uns die Menschenrechte nur ungenügend Schutz gegen die Logik der statistischen Datenverarbeitung und des präventiven Risikomanagements. Wichtig bleibt daher die Sichtbarmachung der Logik, die hinter den Daten steckt, und die Aufhebung der Geheimhaltung bei der Datenverarbeitung, um so überhaupt erst die Grundlagen für die Ausübung der Menschenrechte zu schaffen.

Verantwortliches Wissen umfasst eine Analyse der Wissenslücken, die die Behörden, die sich mit Menschenhandel auseinandersetzen, selber schaffen. Die Formen von Ignoranz und Geheimhaltung – z. B. über die Art der Datennutzung durch Grenzschutzbeamte – und von Unsicherheit in Bezug auf die Behandlung von Individuen treten in diesem Prozess zu Tage. Lösen lässt sich dies nicht einfach durch mehr Wissen. Vielmehr braucht es Vertrauen und Empathie. Einfach mehr Wissen führt letzten Endes nicht unbedingt zu besserem Wissen oder Handeln.

1. EINLEITUNG

Eine rechtsbasierte Sammlung und Analyse von Daten zum Menschenhandel ist ein wichtiges Instrument zur Vertiefung des Wissens und zu einer besseren Erfassung von Trends und Mustern auf nationaler, regionaler und internationaler Ebene. Zudem erlaubt die Sammlung und Analyse dieser Daten eine Setzung von Referenzwerten, anhand derer die Mitgliedstaaten der Europäischen Union Fortschritte bei der Umsetzung nationaler Richtlinien, Strategien und Programme messen können.

Häufig ist der Menschenhandel eine grenzüberschreitende Straftat und verlangt daher die Zusammenarbeit und Koordination zwischen Mitgliedstaaten sowie zwischen Mitgliedstaaten und internationalen und regionalen Institutionen. Zur Verbesserung der internationalen Kooperation und Koordination muss daher die formelle und informelle Zusammenarbeit gefördert werden, z. B. durch die Umsetzung von Verfahren zur Kommunikation und zum Austausch von Informationen und Daten.

Dies setzt eine Verarbeitung von Daten im großen Maßstab voraus, oft auch unter Einbezug personenbezogener Daten. Somit entstehen Risiken für die Wahrung der Privatsphäre von Betroffenen des Menschenhandels und des Rechts auf Achtung ihres Privat- und Familienlebens (Artikel 8 der Europäischen Menschenrechtskonvention). Maßnahmen gegen den Menschenhandel lassen sich daher nicht ohne eine effektive Strategie zum Datenschutz umsetzen.

Zudem werden die Daten der von Menschenhandel Betroffenen nicht nur im Rahmen der Zusammenarbeit von Polizei- und Justizbehörden bei Ermittlungen und bei der Organisation nationaler und transnationaler Unterstützungsleistungen gesammelt, sondern auch zu anderen Zwecken von Regierungen, zwischenstaatlichen Institutionen, Nichtregierungsorganisationen (NROs) und Privatunternehmen erfasst. Darüber hinaus dient die Sammlung von Daten auch kommerziellen Interessen privater Unternehmen. Zivilgesellschaftliche Organisationen, die Beratungen für Betroffene des Menschenhandels anbieten, sehen sich mit multidisziplinären Anforde-

rungen für die Erfassung von personenbezogenen Daten von vom Menschenhandel betroffenen Personen konfrontiert. Einerseits sind sie durch ihre (staatlichen) Geldgeber zur Weitergabe von Informationen gehalten, die ihre soziale Arbeit dokumentiert, andererseits müssen sie Hilfesuchende bei den Sozial- und Gesundheitssystemen registrieren, um Zugang zu finanzieller und anderweitiger Unterstützung für vom Menschenhandel Betroffene zu erhalten. In beiden Fällen ist die Speicherung personenbezogener Daten erforderlich. Auch die Zusammenarbeit mit den Herkunftsländern im Rahmen von Rückkehrprogrammen oder die Nutzung von Cloud-Dienstleistungen kann eine Herausforderung für den Datenschutz darstellen.

Einige der existierenden nationalen Berichterstattungsstellen sammeln ausschließlich anonymisierte/nicht-personenbezogene Daten der von Menschenhandel Betroffenen, andere jedoch legen den Fokus auf die Sammlung personenbezogener Daten von Betroffenen, inklusive detaillierter Angaben zu den gegen sie begangenen Gewaltakten sowie Daten zu den (vermuteten) Täter*innen.

Während der Fokus bei Maßnahmen gegen den Terror auf den Täter*innen liegt, zielt man bei der Bekämpfung des Menschenhandels auf die Erstellung von Profilen der potenziellen und vermuteten Betroffenen. Dieser ‚opferzentrierte Ansatz‘, der häufig als Synonym zu einem menschenrechtsbasierten Ansatz gesehen wird, erscheint allerdings in Hinblick auf die Art der Sammlung von Daten in einem ganz anderen, restriktiveren Licht. Internationale und zwischenstaatliche Organisationen haben Richtlinien und Instrumente zur Sammlung von Daten mit einem starken Fokus auf die Daten der Betroffenen entwickelt⁷. Ernsthafte Bedenken bestehen daher in Bezug auf die Risiken für den Schutz der Privatsphäre und Sicherheit der Betroffenen bei der Sammlung, dem Austausch und anderer Formen der Verarbeitung ihrer personenbezogenen Daten. Der Schutz des Privatlebens und der Identität der Betroffenen ist nicht nur aufgrund der Gefahr von Gewaltakten seitens der Menschenhändler*innen fundamental für den Schutz ihrer körperlichen

7 Siehe Datensammlungsinstrumente entwickelt durch ICMPD und IOM in Kapitel 5 sowie das „DNS, Menschenrechte und Menschenhandelsprogramm“ der Duke University: <http://kenan.ethics.duke.edu/humanrights/dna-human-rights-human-trafficking-sep-13-2/>.

Unversehrtheit, sie ist es auch aufgrund der Gefahr der Stigmatisierung und in Hinblick auf die Möglichkeiten der Opfer, im Herkunftsland bzw. im Aufnahmeland ein neues Leben aufzubauen.

Darüber hinaus sind Personen, die in die Prostitution gehandelt wurden, nicht nur durch Menschenhändler*innen bedroht, sondern auch durch Behörden. Insbesondere in osteuropäischen Ländern werden Sexarbeiter*innen häufig kriminalisiert und laufen daher Gefahr, verhaftet, vor Gericht gestellt und bestraft zu werden. Des Weiteren laufen Personen, die zu kriminellen Handlungen genötigt wurden, Gefahr, strafrechtlich verfolgt und soziale ausgegrenzt zu werden, sobald ihre personenbezogenen Daten durch Behörden und anderer Akteure geteilt werden.

Außerdem kann nicht ausgeschlossen werden, dass Beamte sich an kriminellen Aktivitäten beteiligen. Das Risiko des Datenmissbrauchs ist daher nicht nur durch Kriminelle, sondern auch durch korrupte Beamte gegeben. Gleichzeitig ist es für Hilfesuchende essenziell, darauf vertrauen zu können, dass ihre personenbezogenen Informationen von den Organisationen, bei denen sie nach Unterstützung suchen, streng vertraulich behandelt werden.

Datenschutz-Mechanismen sollten alle Betroffenen von Menschenhandel mit einbeziehen, also Betroffene, die in allen ökonomischen Sektoren ausgebeutet wurden, wie die Sexindustrie, Hausarbeit, Landwirtschaft, Bauindustrie, Lebensmittelindustrie und Pflege.

Dieser hier vorliegende praktische Leitfaden soll die Anwendung von Datenschutzgesetzen bei Maßnahmen gegen den Menschenhandel untersuchen und Empfehlungen aussprechen. In einem ersten Schritt wird ein allgemeiner Überblick über die rechtlichen Instrumente des europäischen Datenschutzes gegeben, dem ein detaillierter Diskurs zur Anwendungen des Konzepts von „sensiblen Daten“ folgt. Im weiteren Verlauf werden spezifische Datenschutzvorkehrungen in Rechtsinstrumenten zur Bekämpfung des Menschenhandels diskutiert. Zuletzt werden die bestehenden rechtlichen und politischen Instrumente auf konkrete Maßnahmen für Praktiker*innen aus nicht-staatlichen, staatlichen und zwischenstaatlichen Sektoren angewendet.

2. ZENTRALE INSTRUMENTE DES DATENSCHUTZES

Dieses Kapitel soll ein Überblick über europäisches Datenschutzrecht bieten und dessen Umsetzung diskutieren.

Die Grundlage aller europäischen Datenschutzinstrumente bildet **Artikel 8 der Europäischen Menschenrechtskonvention (ECHR)** von 1950: das Recht auf Achtung des Privat- und Familienlebens, die den Behörden das Eindringen in die Privatsphäre von Bürger*innen verbietet, sollten nicht ganz bestimmte Bedingungen erfüllt sein. Ähnlich sieht die Charta der Grundrechte der Europäischen Union (2009⁸) den Schutz von personenbezogenen Daten als ein eigenständiges Grundrecht.

Die beiden Hauptinstrumente im Bereich des Datenschutzes sind:

1. Richtlinie 95/46/EG⁹, die sogenannte **Datenschutzrichtlinie**, ist das grundlegende Datenschutzgesetz in der EU-Gesetzgebung. Die Definitionen und Prinzipien der Richtlinie sind der zentrale Referenzpunkt für alle weiteren Instrumente des Datenschutzes. Alle EU-Staaten mussten diese Richtlinie in ihrer nationalen Gesetzgebung umsetzen. Allerdings klammert sie die Verarbeitung von Daten bei der Zusammenarbeit von Polizei und Justiz bei Ermittlungen als Thema aus.¹⁰
2. Aufgrund des beschränkten Wirkungsfelds der Datenschutzrichtlinie entstand 1981 die **Europäische Datenschutzkonvention 108**, auf der die Zusammenarbeit von Polizei und Justiz zwischen 1993 und 2009 basierte, als die Europäische Union (EU) aus drei Säulen bestand. 2008 wurde der separate Rahmenbeschluss (2008/977/JI) verabschiedet,

8 Die Charta wurde 2000 veröffentlicht, aber erst im Jahr 2009 mit dem Lissaboner Vertrag rechtlich bindend.

9 Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr.

10 Artikel 3(2): Diese Richtlinie findet keine Anwendung auf die Verarbeitung personenbezogener Daten, [...] und auf keinen Fall auf Verarbeitungen betreffend die öffentliche Sicherheit, die Landesverteidigung, die Sicherheit des Staates (einschließlich seines wirtschaftlichen Wohls, wenn die Verarbeitung die Sicherheit des Staates berührt) und die Tätigkeiten des Staates im strafrechtlichen Bereich.

der sich allerdings nur mit der grenzüberschreitenden Verarbeitung von Daten befasst. Für die Verarbeitung inländischer Daten bei Straffällen ist die Konvention 108 weiterhin das wichtigste Instrument. Da sie eine Konvention des Europarats ist, ist sie in weitaus mehr europäischen Ländern gültig, als die Datenschutzrichtlinie der EU.

In beiden Instrumenten sind die Schlüsselkonzepte die „personenbezogene Daten“ und die „Verarbeitung personenbezogener Daten“. Sie werden jeweils umfassend definiert.

- „Personenbezogene Daten“ sind alle Informationen über eine bestimmte oder bestimmbare Person („betroffene Person“). Daten sind personenbezogen, sobald sie die Zuordnung von Information zu einer Person ermöglichen, selbst wenn die Person oder Institution, die über diese Information verfügt, diese Verbindung selbst nicht herstellen kann. Damit ist jede Information, die eine Person identifiziert oder anhand derer sich eine Person identifizieren und von anderen Personen unterscheiden lässt, eine personenbezogene Information.
- „Verarbeitung personenbezogener Daten“ („Verarbeitung“) bedeutet jeder Zugriff auf personenbezogene Daten, darunter auch deren Erhebung, Aufnahme, Speicherung, Aufspürung, Einsicht, Nutzung, Übertragung, Verbreitung oder auf andere Weise Verfügbarmachung, Sperrung, Löschung oder Vernichtung.

EU-Datenschutzrichtlinie von 1995

Datenschutz dient dem Schutz des Individuums, dessen Daten verarbeitet werden. Erzielt wird dies durch eine Kombination aus Rechten für das Individuum (in der Sprache des Datenschutzes „Datensubjekt“ genannt)¹¹ und Verpflichtungen für diejenigen, die die Daten verarbeiten (der „Auf-

¹¹ In den folgenden Kapiteln wird auch der Begriff ‚betroffene Person‘ gleichbedeutend mit ‚Datensubjekt‘ benutzt.

tragsverarbeiter“) bzw. diejenigen, die diese Verarbeitung kontrollieren („für die Verarbeitung Verantwortliche“).

Kurz gesagt definiert die Richtlinie 95/46/EG die Verarbeitungsbedingungen für personenbezogene Daten. Sie wurde 1995 vor allem mit zwei Zielen verabschiedet:

- dem Schutz der Privatsphäre in Hinblick auf die Verarbeitung personenbezogener Daten
- der Garantie des freien Flusses personenbezogener Daten zwischen den Mitgliedstaaten

Auf der Richtlinie bauen sämtliche Datenschutzstandards der EU-Gesetzgebung auf. Sie umfasst alle zentralen Elemente der Europäischen Menschenrechtskonvention¹², insbesondere Artikel 8 zur Achtung des Privat- und Familienlebens. Sie findet gleichermaßen auf den öffentlichen wie den privaten Sektor Anwendung, gilt also für NROs, zwischenstaatliche Organisationen (IROs) und Unternehmen (auch multinationale), wann immer die für die Verarbeitung verantwortliche Person zur Verarbeitung von Daten Kapazitäten innerhalb der EU nutzt. Allerdings findet sie keine Anwendung auf die Kooperation von Polizei- und Justizbehörden bei der Verfolgung von Straftaten.

Die Richtlinie selbst beinhaltet keine direkten Verpflichtungen für Personen oder Unternehmen.¹³ Stattdessen fordert sie, dass alle EU-Mitgliedstaaten Gesetze zur Verarbeitung von personenbezogenen Daten verabschieden, die die in der Richtlinie dargelegten Mindeststandards erfüllen.¹⁴ Alle EU-Mitgliedstaaten haben die Richtlinie umgesetzt. Sie verpflichtet alle Staaten auch zum Aufbau einer Kontrollstelle (Regulierungsbehörde: die Datenschutzbehörde eines Landes).

12 Erwägung 1 der Datenschutzrichtlinie.

13 EU Richtlinien richten sich an die Mitgliedstaaten und sind für die Bürger*innen im Prinzip nicht rechtlich bindend. Die Mitgliedstaaten müssen diese Richtlinien dann in nationales Recht umsetzen.

14 Erwägung 69 und Artikel 5 der Datenschutzrichtlinie.

Artikel 29 der Richtlinie verlangt den Aufbau einer Experten*innengruppe bestehend aus Repräsentant*innen der Datenschutzbehörden der Mitgliedstaaten, der Gemeinschaftsinstitutionen sowie der Kommission. Sie hat beratenden Status und handelt unabhängig.¹⁵

Die Richtlinie basiert auf sieben Prinzipien, die innerhalb der EU harmonisiert werden sollen:¹⁶

Prinzipien des Datenschutzes

- **Zweck:** Daten sollten ausschließlich zu den genannten Zwecken verarbeitet werden.
- **Einwilligung:** Personenbezogene Daten sollten nicht ohne Einwilligung der betroffenen Person weitergegeben oder mit Dritten geteilt werden.
- **Sicherheit:** Erhobene Daten sollten sicher aufbewahrt und vor möglichem Missbrauch, Diebstahl oder Verlust gesichert werden.
- **Benachrichtigung:** Betroffene Personen sollten darüber benachrichtigt werden, wer über sie Daten sammelt.
- **Weitergabe:** Personen, deren personenbezogene Daten gesammelt werden, sollten erfahren welche Institution diese Daten sammelt.
- **Zugang:** Betroffenen Personen sollte Zugang zu den über sie gesammelten Daten gewährt werden und die Korrektur falscher Daten sollte ihnen möglich sein.
- **Rechenschaftspflicht:** Betroffene Personen sollten von den für die Verarbeitung Verantwortlichen Rechenschaft über die Einhaltung der genannten Prinzipien verlangen können.

Zusammenfassend verlangen diese Prinzipien, dass personenbezogene Daten nicht ohne Wissen oder eindeutige Zustimmung der betroffenen Person genutzt werden sollten. Sie sollten den Zwecken entsprechen, für die

15 Für weitere Informationen zu deren Aktivitäten siehe: http://ec.europa.eu/justice/policies/privacy/workinggroup/index_en.htm.

16 Leitlinien zur Folgenabschätzung SEK (2012)72 final, Anhang 1, S. 9; http://ec.europa.eu/justice/data-protection/document/review2012/sec_2012_72_en.pdf.

sie gespeichert sind, dafür erheblich sein und dürfen nicht darüber hinausgehen. Darüber hinaus hat die Verarbeitung von Daten inklusive ihrer Weitergabe sorgfältig zu geschehen. Dieser auf Prinzipien basierende Ansatz erlaubt den Mitgliedstaaten die Implementierung der notwendigen Maßnahmen bei gleichzeitiger Rücksichtnahme auf lokale Traditionen und Sensibilitäten sowie auf die Bedürfnisse bestimmter Sektoren.

Übersicht über relevante Bestimmungen

Im Folgenden werden einige der relevanten Bestimmungen der Datenschutzrichtlinie detaillierter diskutiert. Zunächst wird auf die Prinzipien und Bedingungen für die Verarbeitung von Daten, sowie die Reichweite und die Beschränkungen der Richtlinie eingegangen.

Anschließend wird besonders die Kategorie sensibler Daten behandelt sowie die Frage, ob Daten von Betroffenen des Menschenhandels in diese Kategorie fallen oder nicht, insbesondere, wenn es um Personen geht, die für oder im Rahmen der Sexindustrie Betroffene von Menschenhandel werden.

Prinzipien und Bedingungen für die Verarbeitung von Daten

Artikel 6 der Datenschutzrichtlinie enthält eine Liste von Prinzipien für die Qualität von Daten, während Artikel 7 die Bedingungen nennt, unter denen Daten verarbeitet werden können. Artikel 6 schreibt zudem vor, dass die Behörde, die über den Zweck und die Art der Verarbeitung personenbezogener Daten bestimmt (der* die „für die Verarbeitung Verantwortliche“), auch für die Einhaltung der Prinzipien zuständig ist. Der* die für die Verarbeitung Verantwortliche hat auch eine Informationspflicht gegenüber der Person, deren Daten verarbeitet werden (der „betroffenen Person“), unabhängig davon, ob Daten direkt von einer Person¹⁷ oder anderweitig eingeholt werden.¹⁸

¹⁷ Artikel 10 der Datenschutzrichtlinie.

¹⁸ Artikel 11 der Datenschutzrichtlinie.

Artikel 6 der Datenschutzrichtlinie – Prinzipien der Datenqualität

1. Die Mitgliedstaaten sehen vor, dass personenbezogene Daten
 - a) nach Treu und Glauben und auf rechtmäßige Weise verarbeitet werden;
 - b) für festgelegte eindeutige und rechtmäßige Zwecke erhoben und nicht in einer mit diesen Zweckbestimmungen nicht zu vereinbarenden Weise weiterverarbeitet werden. Die Weiterverarbeitung von Daten zu historischen, statistischen oder wissenschaftlichen Zwecken ist im allgemeinen nicht als unvereinbar mit den Zwecken der vorausgegangenen Datenerhebung anzusehen, sofern die Mitgliedstaaten geeignete Garantien vorsehen;
 - c) den Zwecken entsprechen, für die sie erhoben und/oder weiterverarbeitet werden, dafür erheblich sind und nicht darüber hinausgehen;
 - d) sachlich richtig und, wenn nötig, auf den neuesten Stand gebracht sind; es sind alle angemessenen Maßnahmen zu treffen, damit im Hinblick auf die Zwecke, für die sie erhoben oder weiterverarbeitet werden, nichtzutreffende oder unvollständige Daten gelöscht oder berichtigt werden;
 - e) nicht länger, als es für die Realisierung der Zwecke, für die sie erhoben oder weiterverarbeitet werden, erforderlich ist, in einer Form aufbewahrt werden, die die Identifizierung der betroffenen Personen ermöglicht. Die Mitgliedstaaten sehen geeignete Garantien für personenbezogene Daten vor, die über die vorgenannte Dauer hinaus für historische, statistische oder wissenschaftliche Zwecke aufbewahrt werden.
2. Der für die Verarbeitung Verantwortliche hat für die Einhaltung des Absatzes 1 zu sorgen.

Zweck

Das erste Datensammelungsprinzip lautet, dass Daten nur zu dem Zweck genutzt werden sollten, zu dem sie auch gesammelt wurden (Artikel 6(1) (b)). Dies bedeutet, dass die Daten einer Person nur aus folgenden Gründen gesammelt, gespeichert, geteilt etc. werden können:

- **Festgelegte Gründe:** entscheidend für die Gesetzeskonformität.
- **Eindeutige Gründe:** der Grund muss klar und offen benannt werden, damit die betreffende Person versteht, was mit ihren Daten gemacht wurde. Außerdem muss ihr die Möglichkeit gegeben werden, die anwendbaren Rechte zum Schutz der Privatsphäre durchzusetzen.
- **Rechtmäßige Gründe:** steht in Bezug zur Gesetzeskonformität und bedeutet, dass der*die für die Verarbeitung Verantwortliche ein legitimes Motiv zur Verarbeitung personenbezogener Daten haben muss.

Der jeweilige Zweck, aus dem heraus Daten verarbeitet werden, muss vor einer solchen Verarbeitung definiert werden. Darüber hinaus dürfen personenbezogene Daten nicht zu Zwecken benutzt werden, die den Gründen entgegenstehen, aus denen heraus sie ursprünglich gesammelt, gespeichert usw. wurden.

Integraler Bestandteil dieses **Prinzips der Zweckbeschränkung** ist das **Prinzip der Datenqualität**. Dieses legt fest, dass die genutzten Daten den Zwecken, für die sie gespeichert sind, entsprechen müssen, dafür erheblich sein und nicht darüber hinausgehen dürfen (Artikel 6(1)(c)). Dies bezieht sich auf das sogenannte **Datenspeicherungsprinzip**, nach dem nur die Daten verwendet werden dürfen, die zu einem bestimmten legitimen Zweck gebraucht werden (Artikel 6(1)(e)). Mehrmals bereits hat dieses Prinzip zu Diskussionen geführt, ob personenbezogene Daten ein „Verfallsdatum“ haben oder ob Daten ohne zeitliche Begrenzung gespeichert werden dürfen. Unter der Annahme, dass der Zweck, für den Daten relevant waren, weiter besteht, können personenbezogene Daten gespeichert bleiben. Daraus folgt aber, dass wenn der Grund für die Datenverarbeitung erfüllt wurde, diese dann gelöscht, anonymisiert bzw. für andere legitime Zwecke verarbeitet werden sollten.

Das Prinzip der Datenqualität sieht weiterhin vor, dass personenbezogene Daten genau/präzise sein müssen und bei Bedarf aktualisiert werden können. Damit ist der*die für die Verarbeitung Verantwortliche verpflichtet, im Rahmen seiner*ihrer Möglichkeiten dafür zu sorgen, dass nicht genaue/präzise oder unvollständige personenbezogene Daten unter Berücksichti-

gung der Zwecke, zu denen sie ursprünglich gesammelt wurden, gelöscht, berichtigt bzw. anderweitig genutzt werden (Artikel 6(1)(d)). Der Grund dafür ist, dass unvollständige, ungenaue oder falsche Informationen der betroffenen Person erheblichen Schaden zufügen können.

Einwilligung

Ein Schlüsselbegriff ist „Einwilligung“, also „jede Willensbekundung, die ohne Zwang, für den konkreten Fall und in Kenntnis der Sachlage erfolgt und mit der die betroffene Person akzeptiert, daß personenbezogene Daten, die sie betreffen, verarbeitet werden“. Darüber hinaus muss die betroffene Person ihre Einwilligung „ohne jeden Zweifel“ geben.¹⁹ Damit die Einwilligung ohne jeden Zweifel erfolgt, dürfen die Einholung und die Erteilung der Einwilligung keinen Zweifel an der Absicht der Person zur Erteilung ihrer Einwilligung lassen. Der Begriff der Einwilligung geht traditionell mit dem Gedanken einher, dass die Verwendung der eigenen Daten in den Händen des Individuums liegt.

Artikel 7 nennt Kriterien zur legitimen Datenverarbeitung:

Artikel 7: Datenschutzrichtlinie – Kriterien zur Legitimierung der Datenverarbeitung

Die Mitgliedstaaten sehen vor, daß die Verarbeitung personenbezogener Daten lediglich erfolgen darf, wenn eine der folgenden Voraussetzungen erfüllt ist:

- a) Die betroffene Person hat ohne jeden Zweifel ihre Einwilligung gegeben;
- b) die Verarbeitung ist erforderlich für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder für die Durchführung vorvertraglicher Maßnahmen, die auf Antrag der betroffenen Person erfolgen;

¹⁹ Artikel 2(h) und 7(a) der Datenschutzrichtlinie.

- c) die Verarbeitung ist für die Erfüllung einer rechtlichen Verpflichtung erforderlich, der der für die Verarbeitung Verantwortliche unterliegt;
- d) die Verarbeitung ist erforderlich für die Wahrung lebenswichtiger Interessen der betroffenen Person;
- e) die Verarbeitung ist erforderlich für die Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt und dem für die Verarbeitung Verantwortlichen oder dem Dritten, dem die Daten übermittelt werden, übertragen wurde;
- f) die Verarbeitung ist erforderlich zur Verwirklichung des berechtigten Interesses, das von dem für die Verarbeitung Verantwortlichen oder von dem bzw. den Dritten wahrgenommen wird, denen die Daten übermittelt werden, sofern nicht das Interesse oder die Grundrechte und Grundfreiheiten der betroffenen Person, die gemäß Artikel 1 Absatz 1 geschützt sind, überwiegen.

Diese Voraussetzungen werden jedoch derzeit von den Mitgliedstaaten unterschiedlich interpretiert – einige verlangen grundsätzlich eine schriftliche Einwilligung, andere akzeptieren eine stillschweigende Einwilligung. Wie die Folgenabschätzung zum Schutz personenbezogener Daten der Europäischen Kommission im Jahr 2012 gezeigt hat, wenden auch die nationalen Datenschutzbehörden („DSB“) unterschiedliche Auslegungen des Begriffs Einwilligung an.²⁰ Was also in einem Mitgliedstaat eine zulässige Einwilligung darstellt, hat in anderen keine Rechtsgültigkeit.²¹

Eine Einwilligung ist nur dann zulässig, wenn die betroffene Person wirklich die Wahl dazu hat, ohne Gefahr zu laufen, Täuschung, Einschüchterung, Druck oder wesentlichen negativen Konsequenzen ausgesetzt zu werden, falls sie ihre Einwilligung nicht erteilt. Wenn die Auswirkungen der Erteilung oder Ablehnung der Einwilligung die Entscheidungsfreiheit der Person einschränken, dann erfolgt die Einwilligung nicht freiwillig.²² Dies kann dann der Fall sein, wenn sich die betroffene Person in einem Abhängigkeitsverhält-

²⁰ European Commission Impact Assessment.

²¹ European Commission Impact Assessment, Anhang 1, Seite 13.

²² Artikel 29 Datenschutzgruppe „Opinion 15/2011 on the definition of consent“, 13. Juli 2011, Seite 12; http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf.

nis zu der für die Verarbeitung der Daten verantwortlichen Person befindet – sei es durch die Art des Verhältnisses oder besondere Umstände – und fürchten könnte, dass sie anders behandelt wird, wenn sie die Einwilligung zur Verarbeitung ihrer Daten nicht erteilt, beispielsweise wenn die Einwilligung zur Datenverarbeitung Voraussetzung für weitere Maßnahmen ist. Noch konkreter kann die Gültigkeit der Einwilligung folgendermaßen definiert werden:

- » Eine Einwilligung kann nur dann gültig sein, wenn die betroffene Person eine tatsächliche Wahlmöglichkeit hat und kein Risiko einer Täuschung, Einschüchterung, Nötigung oder beträchtlicher negativen Folgen besteht, wenn sie die Einwilligung nicht erteilt.²³

Diese Beschreibung gilt insbesondere im Fall von Einwilligungen, die angesichts eines drohenden Ausbleibens oder einer qualitativ schlechteren medizinischen Behandlung gegeben wurden und daher nicht als „freiwillig“ erachtet werden können. Dieser Fall könnte problemlos auf andere Hilfeleistungen, wie z. B. psychologischer, sozialer oder rechtlicher Unterstützung übertragen werden. Wenn beispielsweise von Menschenhandel betroffene Personen dem Austausch ihrer persönlichen Daten mit Dritten zustimmen müssen, um so Zugang zu Hilfeleistungen zu erlangen, kann die Zustimmung nicht als freiwillig erachtet werden.

Auch wenn der zeitliche Ablauf zur Einholung der Einwilligung in der Richtlinie nicht festgelegt ist, wird doch eindeutig impliziert, dass als generelle Regel die Einwilligung gegeben werden muss, bevor die Verarbeitung der Daten erfolgt.²⁴ Sofern keine Einwilligung erfolgt ist, dürfen personenbezogene Daten nur dann verarbeitet werden, wenn dies für eines der in Artikel 7 beschriebenen Ziele *notwendig* ist. Dies bedeutet, dass die Person der Verarbeitung ihrer Daten entweder zugestimmt hat oder die Verarbeitung das Kriterium der „Notwendigkeit“ erfüllen muss.

23 Artikel 29 Datenschutzgruppe „Opinion on the definition of consent“, Seite 15.

24 Artikel 29 Datenschutzgruppe „Opinion on the definition of consent“, Seite 9.

Sicherheit

Vorkehrungen zur Wahrung von Vertraulichkeit und Sicherheit sollen dem Schutz personenbezogener Daten dienen – sowohl für den Zeitraum ihrer Speicherung als auch für die Weitergabe oder sonstige Zugangsermöglichung gegenüber Dritten. Die Vorkehrungen gelten für personenbezogene Daten in Papierform ebenso wie in elektronischer Form. Sicherheitsmaßnahmen können in zwei Kategorien unterteilt werden: technische und organisatorische Maßnahmen. Mit technischen Maßnahmen sind generell Maßnahmen gemeint, die der Sicherheit von Daten beim Einsatz von elektronischen Geräten und Ausrüstung dienen, beispielsweise Firewalls, Anti-Virusprogramme, Authentifizierungs- und Autorisierungssysteme. Mit organisatorischen Maßnahmen sind Anweisungen, Richtlinien und interne Verfahren zum Umgang mit personenbezogenen Daten durch die verantwortlichen Personen gemeint. Angesichts der Tatsache, dass sensible Daten, aufgrund ihrer Natur und dem möglichen Schaden für die betroffene Person, besonders zu schützen sind, müssen zusätzliche legale, organisatorische und technische Garantien erwo-gen werden, wie die Datenschutzgruppe bestätigte.²⁵

Kapitel IV der Datenschutzrichtlinie befasst sich mit den Auflagen zur Weitergabe personenbezogener Daten ins nicht-europäische Ausland. Die Kernregelung ist klar: Daten dürfen nur an Drittländer übermittelt werden, „wenn dieses Drittland ein angemessenes Schutzniveau gewährleistet“ (Artikel 25 (1)). Zur Beurteilung der Frage, was ein „angemessenes Schutzniveau“ darstellt, berücksichtigt die Kommission folgende Faktoren:

- die Art der Daten;
- die Zweckbestimmung sowie die Dauer der geplanten Verarbeitung;
- das Herkunfts- und das Endbestimmungsland;
- die in dem betreffenden Drittland geltenden allgemeinen und die den Datenschutz betreffenden Rechtsnormen sowie
- die dort geltenden Landesregeln und Sicherheitsmaßnahmen (Artikel 25(2)).

²⁵ Artikel 29 Datenschutzgruppe „Advice paper on special categories of data (sensitive data)“, Seite 11.

Benachrichtigung und Weitergabe

Personenbezogene Daten sollen gerecht und rechtmäßig verarbeitet werden. „Gerecht“ bedeutet, dass die betroffene Person verlässliche Informationen zur Verarbeitung ihrer personenbezogenen Daten erhält. Die für die Datenverarbeitung verantwortliche Person ist auch dafür zuständig, sowohl die betroffene Person als auch die Kontrollstelle informiert zu halten.

Benachrichtigung der betroffenen Person

Transparenz gilt weithin als eines der Kernprinzipien bei der Verarbeitung personenbezogener Daten. Dem Recht auf Information des „Datensubjekts“ wird durch die Informationspflicht der für die Datenverarbeitung verantwortlichen Person Rechnung getragen. Laut Artikel 10 und 11 der Richtlinie muss diese Information folgende Aspekte umfassen: die Identität der für die Verarbeitung verantwortlichen Person, die Zweckbestimmungen der Verarbeitung, die Empfänger*innen oder Kategorien der Empfänger*innen der Daten, die Angabe, ob die Beantwortung der Fragen obligatorisch oder freiwillig ist (einschließlich einer Erklärung zu den möglichen Folgen einer unterlassenen Beantwortung), das Recht auf Auskunft und Berichtigung der eigenen personenbezogenen Daten sowie jegliche weitere Informationen, „sofern sie [...] notwendig sind“ (Artikel 10).

Wenn personenbezogene Daten nicht direkt von der betroffenen Person, sondern von Dritten eingeholt werden, muss die betroffene Person über die Speicherung dieser Daten durch die für die Verarbeitung verantwortliche Person informiert werden. Beabsichtigt die für die Verarbeitung verantwortliche Person eine Offenlegung personenbezogener Daten gegenüber Dritten, ist die betroffene Person im Vorfeld hierüber zu informieren (Artikel 11(1)).

Es bestehen eine Reihe von Ausnahmen hinsichtlich der Informationspflicht gegenüber der betroffenen Person, beispielsweise wenn die Informierung der betroffenen Person unmöglich ist oder einen unverhältnismäßigen Aufwand seitens der für die Verarbeitung verantwortlichen Person erfordert oder wenn die

Speicherung oder Weitergabe der personenbezogenen Daten zur Einhaltung einer konkreten bestehenden Gesetzesregelung notwendig ist (Artikel 11(2)).

Benachrichtigung der Kontrollstelle

Bis auf die von nationalen Gesetzen vorgesehenen Ausnahmen müssen die für die Verarbeitung Verantwortlichen den zuständigen Datenschutzbehörden folgende Informationen vor Beginn jedweder Datenverarbeitung vorlegen:

- den Namen und die Anschrift der für die Verarbeitung verantwortlichen Person;
- die Zweckbestimmung(en) der Verarbeitung;
- eine Beschreibung der Kategorie(n) der betroffenen Personen und der diesbezüglichen Daten;
- die Empfänger*innen oder Kategorien von Empfänger*innen, denen die Daten mitgeteilt werden könnten;
- jegliche geplante Datenübermittlung in Drittländer und
- eine allgemeine Beschreibung der Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.²⁶

Diese Benachrichtigungen sind für jedermann einsehbar (Artikel 21). Die Vorgabe dient der Gewährleistung der Datenverarbeitungs-Transparenz innerhalb eines Mitgliedstaats. Ebenfalls bietet sie Einzelpersonen die Möglichkeit, sich zu informieren und ihre Persönlichkeitsrechte im Rahmen der gültigen Datenschutzbestimmungen geltend zu machen.

Recht auf Selbstauskunft

Das Recht auf Selbstauskunft ermöglicht es Einzelpersonen, die Verarbeitung ihrer personenbezogenen Daten zu überprüfen. Laut Artikel 12 haben sie das Recht auf folgende Auskünfte:

²⁶ Artikel 18 und 19 der Datenschutzrichtlinie.

- die tatsächliche Verarbeitung ihrer personenbezogenen Daten;
- die Zweckbestimmung dieser Verarbeitung;
- die Herkunft und den Inhalt der betreffenden Daten;
- die Offenlegung dieser Daten gegenüber Dritten.

Das Recht auf Selbstauskunft beinhaltet ebenfalls, nicht zutreffende oder unvollständige Daten zu korrigieren, zu löschen oder ihre Weitergabe zu verhindern. Darüber hinaus muss den Datensubjekten die Ausübung dieser Rechte unkompliziert möglich sein: frei und ungehindert in angemessenen Abständen ohne unzumutbare Verzögerung oder übermäßige Kosten. Außerdem steht den Menschen das Recht zu, der Verarbeitung ihrer Daten jederzeit zu widersprechen (Artikel 14(a)).

Das Recht auf Auskunft, Berichtigung und Widerspruch ist allgemein gehalten, ohne die Wege zu konkretisieren, über die diese Rechte tatsächlich auszuüben sind. Ebenso wenig legt die Richtlinie Fristen für die Beantwortung von Anfragen fest oder macht Angaben zur Höhe der Kosten des Rechts auf Berichtigung, Löschung oder Sperrung der Daten.²⁷

Artikel 13 definiert die Fälle, in denen die Rechte der betroffenen Person ausgesetzt oder eingeschränkt werden können, insbesondere zur Gewährleistung der Sicherheit des Staates, der Landesverteidigung, der öffentlichen Sicherheit, der Verfolgung von Straftaten, sofern ein wichtiges wirtschaftliches oder finanzielles Interesse eines Mitgliedstaats oder der Europäischen Union vorliegt oder zum Schutz der betroffenen Person.

Rechenschaftspflicht

Die Richtlinie schreibt jedem der Mitgliedstaaten die Einrichtung einer Kontrollstelle oder „Datenschutzbehörde“ (DSB) vor, um die Einhaltung seiner Datenschutzgesetze zu überwachen (Artikel 28). Der Europäische Gerichtshof hat die Bedeutung des Begriffs „Unabhängigkeit“ der Daten-

²⁷ European Commission Impact Assessment, Anhang 2, Seite 32.

schutzbehörden klargestellt, indem er betonte, dass diese keiner staatlichen Aufsicht unterstellt werden können.²⁸ Die Kontrollstellen verfügen über Untersuchungsbefugnisse und Einwirkungsbefugnisse, wie die Befugnis, die Sperrung, Löschung und Vernichtung von Daten oder das vorläufige oder endgültige Verbot einer Verarbeitung anzuordnen (Artikel 28(3)).

Das Recht auf Vergessenwerden

Das Recht auf Vergessenwerden umfasst das Recht einer jeden Person, ihre Daten nicht weiter zu verarbeiten oder zu löschen, wenn sie für die Zweckbestimmung, für die sie erhoben wurden, bzw. für andere rechtmäßige Zwecke nicht länger benötigt werden. Indirekt wird es von der geltenden Datenschutzrichtlinie getragen, in der die für die Verarbeitung Verantwortlichen verpflichtet werden, personenbezogene Daten dann zu löschen, wenn sie für rechtmäßige Zwecke nicht länger benötigt werden (Artikel 6).

Die Richtlinie sieht ebenfalls einen aktiven Durchsetzungsmechanismus vor, in dem sie den Menschen das Recht auf Auskunftserteilung über die Frage gewährt, ob und welche ihrer personenbezogenen Daten verarbeitet werden. Gleichfalls kann eine betroffene Person die Berichtigung, Löschung oder Sperrung von Daten fordern, wenn diese beispielsweise nicht länger zutreffend sind, die Person ihre Zustimmung widerruft oder weil die angemessene Speicherungsfrist verstrichen ist (Artikel 12). In der Praxis aber ist es für Einzelpersonen nicht einfach, diese Rechte gegenüber der für die Datenverarbeitung verantwortlichen Person durchzusetzen.

In politischen Debatten wird zugunsten eines sichtbareren und expliziteren Rechts auf Vergessenwerden argumentiert. Tatsächlich ist ein solches Recht in der geplanten Reform der Richtlinie aufgenommen worden²⁹.

28 Europäischer Gerichtshof, Rechtssache C-518/07, Europäische Kommission gegen Bundesrepublik Deutschland, Urteil vom 9. März 2010.

29 2012 hat die EU Kommission ein Gesetzespaket zur Reformierung des Europäischen Datenschutzes verabschiedet, einschließlich eines Vorschlags für eine neue Regulierung (COM(2012)11 final) und Richtlinie (COM(2012)10final).

Geltungsbereich

Artikel 1(1) der Datenschutzrichtlinie definiert den Geltungsbereich:

- » Die Mitgliedstaaten gewährleisten nach den Bestimmungen dieser Richtlinie den Schutz der Grundrechte und Grundfreiheiten und insbesondere den Schutz der Privatsphäre natürlicher Personen bei der Verarbeitung personenbezogener Daten.

Die Richtlinie gilt für natürliche Personen, also für Menschen. Das Recht auf Schutz der personenbezogenen Daten ist in diesem Sinne universell und nicht auf Staatsbürger*innen oder Anwohner*innen eines bestimmten Landes beschränkt.³⁰ Explizit wird dies in dem Erwägungsgrund 2 der Datenschutzrichtlinie verdeutlicht, in dem es heißt: „[Die] Datenverarbeitungssysteme stehen im Dienste des Menschen“ und „haben, ungeachtet der Staatsangehörigkeit oder des Wohnorts der natürlichen Personen, deren Grundrechte und -freiheiten und insbesondere deren Privatsphäre zu achten“.

Nationale Gesetzgebungen erläutern das Konzept der individuellen Persönlichkeit noch präziser, nämlich als die Fähigkeit, Subjekt von rechtlichen Beziehungen zu sein, die mit der Geburt des Individuums beginnen und mit seinem Tod enden.³¹ Personenbezogene Daten sind also Daten über bestimmte oder bestimmbare *lebende* Menschen. Im Prinzip kann die Richtlinie daher nicht auf die Daten von Verstorbenen angewandt werden.³²

Die Richtlinie reguliert neben elektronischen (computerisierten) Daten auch die schriftliche oder mündliche Kommunikation. Sie gilt sowohl für Daten,

30 Artikel 29 Datenschutzgruppe „Opinion on the concept of personal data“, Seite 21.

31 Artikel 29 Datenschutzgruppe „Opinion on the concept of personal data“, Seite 22.

32 In einigen Fällen können die Daten von Verstorbenen dennoch indirekten Schutz erhalten, beispielsweise wenn es der für die Verarbeitung der Daten verantwortlichen Person nicht möglich ist, sicherzustellen, ob die betroffene Person noch am Leben oder bereits gestorben ist, oder in Fällen, in denen die Informationen über Tote auch Aufschluss über lebende Personen geben (z. B. über Erkrankungen). Informationen über Verstorbene können neben den Datenschutzbestimmungen auch durch andere Regelungen geschützt sein, wie zum Beispiel durch die Schweigepflicht des medizinischen Personals, die nicht mit dem Tod des*der Patient*in endet.

die automatisiert verarbeitet wurden (z.B. Computerdatenbanken zu Kund*innen), sowie für nicht automatisiert verarbeitete Daten, die in einem Ablagesystem gespeichert sind oder gespeichert werden sollen.³³

Einige Bestimmungen haben ein gewisses Maß an Flexibilität, sodass sich der Schutz der persönlichen Rechte auf der einen Seite und die legitimen Interessen der für die Verarbeitung der Daten Verantwortlichen, von Dritten und des öffentlichen Interesses auf der anderen Seite die Waage halten.³⁴

Internationale Organisationen

Die Richtlinie gilt sowohl für den öffentlichen Bereich als auch für den Privatsektor, einschließlich NROs, Unternehmen und IROs.³⁵ Zudem gelten die Bestimmungen nicht nur dann, wenn die für die Datenverarbeitung verantwortliche Person in der EU ansässig ist oder dort agiert, sondern immer, wenn sie Einrichtungen innerhalb der EU zur Verarbeitung personenbezogener Daten nutzt. Dies ist insbesondere für internationale Organisationen relevant. Wenn beispielsweise ein ausländisches Unternehmen oder eine internationale Organisation keine Niederlassung in der EU, wohl aber ein Rechenzentrum innerhalb der Europäischen Union hat, muss es sich an die Gesetze der betreffenden Mitgliedstaaten (und damit indirekt auch an die Richtlinie) halten.

Dennoch besteht eines der Probleme, auf das die Kommission in ihrer Mitteilung „Gesamtkonzept für den Datenschutz in der Europäischen Union“ hinweist, darin, dass es der für die Verarbeitung der Daten verantwortlichen Person und der Kontrollstelle nicht immer ersichtlich ist, welcher der Mitgliedstaaten zuständig ist und welches der Gesetze gilt, wenn mehrere Mitgliedstaaten beteiligt sind. Dies ist beispielsweise dann der Fall, wenn ein multinationales Unternehmen in mehreren Mitgliedstaaten ansässig ist oder

33 Artikel 3(1) der Datenschutzrichtlinie. Beispielsweise klassische Akten, wie alphabetisch nach Namen geordnete Klienten-Karteien.

34 Artikel 29 Datenschutzgruppe „Opinion on the concept of personal data“, Seite 5.

35 European Commission Impact Assessment, Anhang 1, Seite 10.

wenn die für die Datenverarbeitung verantwortliche Person nicht in der EU ansässig ist, ihre Dienste aber Einwohner*innen der EU zur Verfügung stellt.³⁶

Einschränkungen

In zwei Bereichen findet die Datenschutzrichtlinie keine Anwendung:

- Die Richtlinie gilt nicht für die Ausübung von Tätigkeiten, die nicht in den Geltungsbereich des Gemeinschaftsrechts fallen. Die hierzu gehörenden Tätigkeiten betreffen „die öffentliche Sicherheit, die Landesverteidigung, die Sicherheit des Staates (einschließlich seines wirtschaftlichen Wohls, wenn die Verarbeitung die Sicherheit des Staates berührt) und die Tätigkeiten des Staates im strafrechtlichen Bereich“³⁷, hier haben die Nationalstaaten das Vorrecht.
- Die Richtlinie gilt nicht für die Verarbeitung personenbezogener Daten, „die von einer natürlichen Person zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten vorgenommen wird“.³⁸ Zu solchen Tätigkeiten zählen beispielsweise die Nutzung einer computerisierten Tabelle zur Anlage einer Mailing-Liste für Einladungen zu einer Geburtstagsparty oder Ankündigung eines erlangten Abschlusses.

Zudem sind die Mitgliedstaaten aufgefordert, Ausnahmen für die Verarbeitung personenbezogener Daten vorzusehen, „die allein zu journalistischen, künstlerischen oder literarischen Zwecken erfolgt“, um die Freiheit der Meinungsäußerung mit dem Recht auf Privatsphäre in Einklang zu bringen.³⁹

36 KOM(2010) 609 endgültig – Mitteilung der Europäischen Kommission „Gesamtkonzept für den Datenschutz in der Europäischen Union“, Brüssel, Seite 11. Als Gründe für die Mitteilung nennt die Europäische Kommission unter anderem das gestiegene Risiko für die Privatsphäre und den Schutz der personenbezogenen Daten im Zusammenhang mit der Nutzung des Internets (beispielsweise die Seiten sozialer Netzwerke und Cloud Computing) sowie die Tatsache, dass die Möglichkeiten des Sammelns personenbezogener Daten immer komplexer und schwieriger aufspürbar geworden sind. http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_de.pdf.

37 Artikel 3(2) Datenschutzrichtlinie.

38 Ebd.

39 Artikel 9 der Datenschutzrichtlinie.

Drittländer

Eine wichtige Funktion der Richtlinie ist die Einschränkung der Weitergabe von personenbezogenen Daten in nicht-europäische Länder, um zu verhindern, dass durch die Verlagerung der Datenverarbeitung ins Nicht-EU-Ausland die Regelungen umgangen werden. In Artikel 25(1) der Datenschutzrichtlinie heißt es:

- » Die Mitgliedstaaten sehen vor, daß die Übermittlung personenbezogener Daten, die Gegenstand einer Verarbeitung sind oder nach der Übermittlung verarbeitet werden sollen, in ein Drittland [...] zulässig ist, wenn dieses Drittland ein angemessenes Schutzniveau gewährleistet.⁴⁰

Übermittlungen in Länder, die das Kriterium der Angemessenheit – also das Kriterium, das über die Frage entscheidet, ob ein Land ein angemessenes Schutzniveau vorsieht – nicht erfüllen, sind nur zulässig, sofern die Herkunftspartei zusätzliche Maßnahmen einleitet, um den angemessenen Schutz der Daten im Ausland zu garantieren. Die nationalen Datenschutzbehörden der EU-Mitgliedstaaten entscheiden in letzter Instanz, ob die Übermittlung zulässig ist oder nicht.⁴¹

Sanktionen

Die Richtlinie gewährleistet die Einhaltung dieser Bestimmungen durch Verfahrensvorschriften zur Haftung, Sanktionen, Rechtsbehelfe und durch die Kontrollstellen.⁴² Verstöße können zwei Haftungsebenen betreffen: Zum einen können sie Sanktionen der nationalen Datenschutzbehörden oder einer gerichtlichen Instanz nach sich ziehen. Die Richtlinie verpflichtet jeden

40 Aktuelle Entscheidungen zur Angemessenheit des Schutzniveaus werden hier auf Englisch veröffentlicht: http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm.

41 Artikel 26(2) der Datenschutzrichtlinie.

42 Kapitel III der Datenschutzrichtlinie.

der Mitgliedstaaten zur Festlegung von Sanktionen bei Verstößen gegen ihre Vorschriften.⁴³ Diese Sanktionen können in Form von Bußgeldern oder Haftstrafen ergehen. Zum anderen können sie zu zivilrechtlichen Haftungsansprüchen seitens der Person führen, deren Rechte verletzt wurden. Die Richtlinie fordert die Mitgliedstaaten auf, dafür Sorge zu tragen:

- » daß jede Person, der wegen einer rechtswidrigen Verarbeitung oder jeder anderen mit den einzelstaatlichen Vorschriften zur Umsetzung dieser Richtlinie nicht zu vereinbarenden Handlung ein Schaden entsteht, das Recht hat, von dem für die Verarbeitung Verantwortlichen Schadenersatz zu verlangen.⁴⁴

Trotzdem verhindern die Rechtssysteme mehrerer Mitgliedstaaten in der Praxis die Möglichkeit, Schadenersatz bei Verstößen gegen die Datenschutzrechte zu fordern. Schuld ist das Zusammenkommen mehrerer Faktoren wie der Beweislast, der Schwierigkeiten bei der Schadensfestsetzung und der mangelnden Unterstützung durch die Kontrollstellen.⁴⁵

Sensible Daten

Von besonderem Interesse aus der Perspektive der vom Menschenhandel betroffenen Personen ist die Kategorie der „sensiblen Daten“. Sowohl das Übereinkommen 108 als auch die Datenschutzrichtlinie basieren auf der Annahme, dass bestimmte Kategorien personenbezogener Daten ein größeres Risiko für den Persönlichkeitsbereich einer Person bergen, als ‚reguläre‘ personenbezogene Daten und daher besonderen Schutzes bedürfen. Die Verarbeitung solcher Daten ist daher strengeren Einschränkungen unterworfen. Diese Sonderdatenkategorie wird auch unter dem Begriff „sensible Daten“ geführt. Artikel 8(1) definiert diese als:

43 Artikel 24 der Datenschutzrichtlinie.

44 Artikel 23(1) der Datenschutzrichtlinie.

45 Agentur der Europäischen Union für Grundrechte (FRA): „Datenschutz in der Europäischen Union: die Rolle der nationalen Datenschutzbehörden. Stärkung der Grundrechte-Architektur in der EU – Teil II“ (2010), Seite 8; http://fra.europa.eu/sites/default/files/tk3109265dec_de_web.pdf.

- » Daten, aus denen die rassische und **ethnische Herkunft**, politische Meinungen, religiöse oder philosophische Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie von Daten über **Gesundheit** oder **Sexualleben**. (eigene Hervorhebung)

Mit wenigen Ausnahmen unter bestimmten Umständen und unter Einhaltung von Garantien ist die Verarbeitung sensibler Daten grundsätzlich verboten (Artikel 8 der Richtlinie). Ausnahmen sind beispielsweise medizinische Gründe oder die Verarbeitung der Daten von Mitgliedern einer Vereinigung oder Gewerkschaft. Wenn keine der aufgelisteten Ausnahmen zutrifft und die betroffene Person ihre konkrete und informierte Zustimmung nicht freiwillig gegeben hat, ist eine Ausnahme des Verbots der Verarbeitung sensibler Daten nur dann gerechtfertigt, wenn:

- eine entsprechende Rechtsgrundlage besteht,
- ein wichtiges öffentliches Interesse vorliegt und
- angemessene Garantien vorgesehen sind.

Artikel 8 Datenschutzrichtlinie – Sensible Daten

1. Die Mitgliedstaaten untersagen die Verarbeitung personenbezogener Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie von Daten über Gesundheit oder Sexualleben.
2. Absatz 1 findet in folgenden Fällen keine Anwendung:
 - a) Die betroffene Person hat ausdrücklich in die Verarbeitung der genannten Daten eingewilligt, es sei denn, nach den Rechtsvorschriften des Mitgliedstaats kann das Verbot nach Absatz 1 durch die Einwilligung der betroffenen Person nicht aufgehoben werden; oder
 - b) die Verarbeitung ist erforderlich, um den Rechten und Pflichten des für die Verarbeitung Verantwortlichen auf dem Gebiet des Arbeitsrechts Rechnung zu tragen, sofern dies aufgrund von einzelstaatlichem Recht, das angemessene Garantien vorsieht, zulässig ist; oder

- c) die Verarbeitung ist zum Schutz lebenswichtiger Interessen der betroffenen Person oder eines Dritten erforderlich, sofern die Person aus physischen oder rechtlichen Gründen außerstande ist, ihre Einwilligung zu geben; oder
 - d) die Verarbeitung erfolgt auf der Grundlage angemessener Garantien durch eine politisch, philosophisch, religiös oder gewerkschaftlich ausgerichtete Stiftung, Vereinigung oder sonstige Organisation, die keinen Erwerbszweck verfolgt, im Rahmen ihrer rechtmäßigen Tätigkeiten und unter der Voraussetzung, daß sich die Verarbeitung nur auf die Mitglieder der Organisation oder auf Personen, die im Zusammenhang mit deren Tätigkeitszweck regelmäßige Kontakte mit ihr unterhalten, bezieht und die Daten nicht ohne Einwilligung der betroffenen Personen an Dritte weitergegeben werden; oder
 - e) die Verarbeitung bezieht sich auf Daten, die die betroffene Person offenkundig öffentlich gemacht hat, oder ist zur Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche vor Gericht erforderlich.
3. Absatz 1 gilt nicht, wenn die Verarbeitung der Daten zum Zweck der Gesundheitsvorsorge, der medizinischen Diagnostik, der Gesundheitsversorgung oder Behandlung oder für die Verwaltung von Gesundheitsdiensten erforderlich ist und die Verarbeitung dieser Daten durch ärztliches Personal erfolgt, das nach dem einzelstaatlichen Recht, einschließlich der von den zuständigen einzelstaatlichen Stellen erlassenen Regelungen, dem Berufsgeheimnis unterliegt, oder durch sonstige Personen, die einer entsprechenden Geheimhaltungspflicht unterliegen.
4. Die Mitgliedstaaten können vorbehaltlich angemessener Garantien aus Gründen eines wichtigen öffentlichen Interesses entweder im Wege einer nationalen Rechtsvorschrift oder im Wege einer Entscheidung der Kontrollstelle andere als die in Absatz 2 genannten Ausnahmen vorsehen.
5. Die Verarbeitung von Daten, die Straftaten, strafrechtliche Verurteilungen oder Sicherungsmaßnahmen betreffen, darf nur unter behördlicher Aufsicht oder aufgrund von einzelstaatlichem Recht, das angemessene Garantien vorsieht, erfolgen [...].

Wie bereits erwähnt, ist das Konzept der personenbezogenen Daten breit auszulegen und bezieht sich auf jegliche Informationen über eine bestimmte oder bestimmbare Person. Personenbezogene Daten können direkt oder indirekt sensibel sein. Direkt sensible Daten sind *per se* sensibler Natur, wie beispielsweise ein Register, in dem neben Namen und Adresse auch die ethnische Herkunft einer Person erfasst wird. Indirekt sensible Daten gehören nicht einer der als sensibel erachteten Kategorien an, können jedoch als solche aus der Eintragung abgeleitet werden. So beispielsweise im Fall der Verwaltung einer Kirchengemeinde, in der die Namen und Anschriften der Mitglieder aufgelistet sind. Als solche handelt es sich hierbei nicht um sensible Daten, aber aufgrund der Tatsache, dass sie in der Verwaltung einer Kirchengemeinde gelistet sind, geben die Daten Auskunft über die religiöse Überzeugung der betroffenen Personen. Entscheidend ist also, dass in diesem Fall der Kontext der Datenerfassung aus den Daten indirekt sensible Daten entstehen lässt.

Gilt das Konzept der „sensiblen Daten“ für die Angaben von Betroffenen von Menschenhandel?⁴⁶

Eine interessante Frage ist natürlich, ob Daten über Betroffene von Menschenhandel in die Kategorie „sensible Daten“ fallen, wie in der Datenschutzrichtlinie definiert. Wichtig ist dies insbesondere angesichts der zunehmenden Bedeutung der Erfassung von Daten nicht nur der Täter*innen, sondern auch der (vermeintlichen) Betroffenen. Außerdem werden personenbezogene Daten der Betroffenen von Menschenhandel von zahlreichen Regierungs- und Nicht-Regierungsorganisationen sowie zwischenstaatlichen Organisationen gespeichert und zwar im Rahmen der Harmonisierung der Datenerhebungsverfahren in der EU und der OSZE-Region, der Rationalisierung der grenzüberschreitenden Unterstützung der Betroffenen von Menschenhandel, der Entwicklung transnationaler Verweisungsmechanismen und der Zunahme der grenzüberschreitenden Zusammenarbeit der Polizei.

46 Das Kapitel über sensible Daten basiert auf den juristischen Untersuchungen von Van der Feltz advocaten (W.I. Koelewijn & R.L. de Graaff), im Auftrag der niederländischen Vereinigung für Frauen und Recht, zur Vereinbarkeit des Gesetzes über die obligatorische Erfassung von Sexarbeiter*innen aus dem Jahr 2009 mit der Datenschutzrichtlinie und ihrer Umsetzung im niederländischen Recht (Wet bescherming persoonsgegevens).

In vielen Fällen betrifft dies sensible Daten, aufgrund derer die Betroffenen von Menschenhandel dem Risiko von Vergeltungsmaßnahmen durch Täter*innen, Strafverfolgung oder Strafvollzug durch die Behörden in den Ländern, in denen Prostituierte kriminalisiert wird, sowie dem sozialen Ausschluss aus ihrem gesellschaftlichen Umfeld ausgesetzt werden könnten.

Aus diesem Grund ist die Frage von großer Relevanz, ob die Daten von Betroffenen des Menschenhandels als sensibel erachtet werden müssen oder nicht.

Das Konzept des „Sexuallebens“

In Anbetracht der in Artikel 8(1) aufgeführten Sonderkategorien, liegt es auf der Hand, dass die Daten der Betroffenen von Menschenhandel für die Sexindustrie durchaus unter Daten zum Sexualleben von Menschen fallen können. Dies führt zu der Frage, was unter „Sexualleben“ im Sinne von Artikel 8(1) der Datenschutzrichtlinie zu verstehen ist.

Der Begriff „Sexualleben“ wird in der Datenschutzrichtlinie oder ihrer Präambel weder definiert noch erläutert. Auch die Rechtsprechung des Europäischen Gerichtshofs liefert keine Interpretation des Konzepts.

Die Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte (EGMR) bietet jedoch einige Leitlinien. In verschiedenen Fällen hat der EGMR Sexualität als einen der intimsten Aspekte der Privatsphäre des Menschen definiert, was bedeutet, dass in einer demokratischen Gesellschaft nur besonders ernste Gründe eine Einmischung durch die Regierung rechtfertigen können.⁴⁷

Insbesondere in Ländern, in denen Prostitution als Arbeit anerkannt ist, könnte man argumentieren, dass die Information über die Prostitution einer

⁴⁷ EGMR, 22. Oktober 1981, Antrag Nr. 7525/76, Dudgeon gegen Großbritannien; EGMR, 22. Oktober 1988, Antrag Nr. 10581/83, Norris gegen Irland.

Person nicht als Angabe zum Sexualleben erachtet werden kann, da sich diese Angabe auf das berufliche Sexualleben und nicht ihre privaten sexuellen Vorlieben oder die sexuelle Orientierung der Person bezieht.⁴⁸

Eine solche Unterscheidung zwischen dem Berufs- und Privatleben einer Person wird in der Rechtsprechung sowohl des Europäischen Gerichtshofs als auch des EGMR nicht unterstützt. In dieser Hinsicht nimmt der Europäische Gerichtshof Bezug auf die Rechtsprechung des EGMR, beispielsweise den Fall *Schecke & Eifert*:

- » Der Umstand, dass sich die veröffentlichten Daten auf berufliche Tätigkeiten beziehen, ist insoweit ohne Belang [...]. Der Europäische Gerichtshof für Menschenrechte hat in Bezug auf die Auslegung von Art. 8 EMRK insoweit entschieden, dass der Begriff „Privatleben“ nicht eng ausgelegt werden darf und dass es „grundsätzlich nicht in Betracht kommt, berufliche Tätigkeiten ... vom Begriff des „Privatlebens“ auszunehmen.“⁴⁹

Der EGMR hat den Begriff des „Privatlebens“ immer weit ausgelegt. Ein Urteil, in dem der EGMR dies klar verdeutlicht, ist der Fall *Niemietz gegen Deutschland*, in dem er unter anderem urteilt:

- » Es scheint [...] keinen prinzipiellen Grund dafür zu geben, warum der Begriff des „Privatlebens“ Handlungen beruflicher oder geschäftlicher Natur ausschließen sollte, denn es ist schließlich im Rahmen ihres beruflichen Lebens, in dem sich der Mehrheit der Bevölkerung wichtige, wenn nicht die meisten, Möglichkeiten bieten in Beziehungen mit der Außenwelt zu treten. Diese Sichtweise wird durch die Tatsache gestützt, dass [...] es nicht immer möglich ist klar zu unterscheiden, welche Handlungen

48 Diese Begründung wäre natürlich noch fragwürdiger in den Fällen, in denen die Personen gegen ihren Willen zur Prostitution gezwungen wurden.

49 EuGH, C-92/09 und C93 / 09 von 9. November 2010 (*Schecke & Eifert*), § 59; siehe auch EuGH, C-456/00 *Österreichischer Rundfunk u. a.*, §§ 73 und 74; EuGH, 8. November 2007, T-194/04, *Bavarian Lager Co. Ltd.* und EGMR, 16. Dezember 1992-A 13710/88, *Niemietz gegen Deutschland*, § 29.

einer Person Teil ihres beruflichen oder geschäftlichen Lebens darstellen und welche nicht. Insbesondere bei Personen, die einen freien Beruf ausüben, kann ihre Arbeit in diesem Zusammenhang einen so wesentlichen Bestandteil ihres Lebens darstellen, dass es unmöglich ist zu wissen, in welcher Eigenschaft sie zu einem gegebenen Zeitpunkt handeln.

Den Schutz durch Artikel 8 aufgrund dessen zu verwehren, dass die beanstandete Maßnahme sich nur auf berufliches Handeln beschränke – wie es die Regierung in dem vorliegenden Fall vorschlug –, könnte darüber hinaus zu einer Ungleichbehandlung führen, bei der ein solcher Schutz nur den Personen zustünde, deren berufliche und nicht berufliche Handlungen derart miteinander verflochten sind, dass eine Unterscheidung zwischen beiden unmöglich ist.⁵⁰

Es muss daher geschlossen werden, dass eine Unterscheidung zwischen dem beruflichen und privaten Sexualleben im Widerspruch zu der Rechtsprechung des Europäischen Gerichtshofs und dem EGMR steht. Beide sehen keinen Grund für eine solche Unterscheidung zwischen beruflichen und persönlichen Handlungen, insbesondere dann nicht, wenn diese eng miteinander verwoben sind. Daraus folgt, dass unter dem Begriff „Sexualleben“ im Sinne von Artikel 8(1) der Datenschutzrichtlinie nicht nur das private, sondern auch das berufliche Sexualleben einer Person zu verstehen ist. Bezüglich der Frage, ob etwas eine Einmischung in die Privatsphäre darstellt, ist die Tatsache, dass es das Berufsleben einer Person betrifft, daher nicht relevant.

Das betrifft auch die (obligatorische) Registrierung von Sexarbeiter*innen, die in einigen Mitgliedstaaten der EU erfolgt. In diesem Zusammenhang ist auch das Urteil des Gerichtshofs im Fall *Khelili gegen die Schweiz* von Bedeutung, bei dem der EGMR entschied, dass die 15 Jahre währende Einstufung einer französischen Frau als „Prostituierte“ in der Computerdatenbank der Genfer Polizei ihr Recht auf Wahrung der Privatsphäre verletzte:

50 EGMR, 16. Dezember 1992, Antrag Nr. 13710/88, Niemietz gegen Deutschland, § 29.

- » Im vorliegenden Fall gelangt der Gerichtshof zu der Einschätzung, dass die Speicherung der Daten der Klägerin mit Bezug auf ihr Berufsleben, das Teil ihres Privatlebens ist, einen Verstoß gegen Artikel 8 der Konvention darstellt, da es sich um personenbezogene Daten einer bestimmten bzw. bestimmbaren Person handelt. Festzustellen bleibt, dass in diesem Zusammenhang zwar die Berufsbezeichnung der Klägerin „Prostituierte“ aus der Datenbank der Polizei gelöscht und durch „Schneiderin“ ersetzt wurde, die strittige Bezeichnung jedoch in den Daten zu zahlreichen Fällen vor den Gerichten des Kantons Genf erhalten blieb.⁵¹

Ein weiterer Aspekt in diesem Fall war, dass der Gerichtshof zu dem Schluss kam, der Vorwurf der rechtswidrigen Prostitution wäre zu vage und allgemein formuliert und stütze sich nicht auf konkrete Beweise. Frau Khelili war nach Schweizer Recht auch nie wegen „rechtswidriger Prostitution“ verurteilt worden.

Voraussetzungen für Ausnahmen zum generellen Verbot der Verarbeitung sensibler Daten

Gemäß Artikel 8(4) ist die Verarbeitung sensibler Daten strengeren Regeln unterworfen und muss:

- aus Gründen eines wichtigen öffentlichen Interesses notwendig sein;
- mit angemessenen Garantien einhergehen;
- eine rechtliche Grundlage haben.⁵²

Ob die Verarbeitung sensibler Daten aus Gründen eines wichtigen öffentlichen Interesses notwendig ist, wird auf Grundlage einzelner Fallentschei-

51 EGMR, 18. Oktober 2011, Antrag Nr. 16188/07, Khelili gegen die Schweiz, § 56 (liegt nur auf Französisch vor). Siehe Presseerklärung (auf Englisch und Französisch): [http://hudoc.echr.coe.int/sites/eng-press/pages/search.aspx?i=003-3714372-4232718#{"itemid":\["003-3714372-4232718"\]}](http://hudoc.echr.coe.int/sites/eng-press/pages/search.aspx?i=003-3714372-4232718#{).

52 Entweder durch eine nationalen Rechtsvorschrift oder eine Entscheidung der Kontrollstelle.

dungen zu prüfen sein. Die Kriterien dieser Beurteilung können jedoch aus Artikel 8(2) der Europäischen Menschenrechtscharta und der zugehörigen Rechtsprechung des EGMR abgeleitet werden.⁵³

- die Verarbeitung dient einem legitimen Zweck;
- die Mittel (z. B. die Verarbeitung sensibler Daten) müssen dem Zweck gegenüber angemessen sein (Grundsatz der Verhältnismäßigkeit);
- andere weniger gravierende Mittel zur Erreichung des Zweckes sind nicht gegeben (Grundsatz der Subsidiarität).

Wenn ein wichtiges öffentliches Interesse besteht, muss folgerichtig geurteilt werden, ob die Verarbeitung sensibler Daten im Sinne dieses Interesses ebenfalls *notwendig* ist. Im Zusammenhang mit dieser „Notwendigkeitsprüfung“ kommt die Europäische Rechtsprechung zu dem Schluss, dass die Mittel (z. B. die Verarbeitung sensibler Daten) dem Zweck angemessen sein und im Verhältnis zu diesem stehen müssen. Darüber hinaus dürfen keine weniger einschneidenden Mittel zur Erreichung des Zwecks zur Verfügung stehen.

Die Datenschutzgruppe sieht die Notwendigkeit gegeben, die Voraussetzung „aus Gründen eines wichtigen öffentlichen Interesses“ klarer zu definieren.⁵⁴ Sie empfiehlt, Artikel 52(1) der EU-Grundrechte-Charta als Vorbild zu nehmen und die Verarbeitung sensibler personenbezogener Daten nur infolge eines Rechtsakts zuzulassen, in dem die Ziele und Gründe (die das wichtige öffentliche Interesse verdeutlichen) der Verarbeitung klar dargelegt werden.

Zuzüglich der Voraussetzung eines wichtigen öffentlichen Interesses müssen angemessene Garantien gegeben werden. Die Angemessenheit dieser Garantien hängt von den Umständen des jeweiligen Falls ab. Die Frage, ob die Garantien tatsächlich „angemessen“ sind, wird sich mit der Zeit verändern, wenn man beispielsweise den technologischen Fortschritt hinsichtlich der Sicherheit personenbezogener Daten berücksichtigt.

⁵³ Siehe beispielsweise EGMR, 4. Dezember 2008, Antrag Nr. 30562/04 und 30566/04, S. und Marper gegen Großbritannien; EGMR, 18. Mai 2010, Antrag Nr. 26839/05, Kennedy gegen Großbritannien.

⁵⁴ Artikel 29 Datenschutzgruppe „Advice paper on special categories of data (sensitive data)“, Seite 11.

Im Fall der Verarbeitung personenbezogener Daten setzt der EGMR höhere Standards in Hinblick auf die (rechtlichen) Garantien, die von Gesetz wegen für den Schutz der Privatsphäre vorzusehen sind.⁵⁵ Diese umfassen unter anderem die Garantie, dass keine weiteren als die unbedingt notwendigen Daten erfasst werden, der Zeitraum der Speicherung beschränkt wird und Vorkehrungen zur Vertraulichkeit getroffen werden. Des Weiteren muss gesetzlich geregelt werden, wer für die Verarbeitung der Daten verantwortlich ist und wer Zugang zu den Daten erhält.

Schlussfolgerung

Hieraus ist zu schließen, dass zumindest die Daten über die Prostitution der Betroffenen von Menschenhandel „sensible Daten“ sind. Dies impliziert, dass bei der Verarbeitung solcher Daten strenge Bedingungen eingehalten werden müssen, um eine Ausnahme des allgemeinen Verbots der Verarbeitung sensibler Daten zu rechtfertigen. Es ist fraglich, ob diese Bedingungen in der Praxis in allen Fällen eingehalten werden, in denen Daten über Betroffene von Menschenhandel gesammelt, gespeichert und ausgetauscht werden.

Hinsichtlich der Daten von Menschenhandelsbetroffenen, die nicht zum Zweck der sexuellen Ausbeutung gehandelt wurden, ist es weniger eindeutig, ob diese sensibler Natur sind und damit strikteren Regelungen unterliegen. Hierfür wäre weitere Forschung notwendig.

Trotzdem können bezüglich der Daten zu Gesundheit und ethnischer Herkunft der Betroffenen von Menschenhandel ähnliche Argumente angeführt werden, unabhängig davon, in welcher Branche sie ausgebeutet werden.

⁵⁵ Siehe beispielsweise EGMR, 4. Dezember 2008, Antrag Nr. 30562/04 und 30566/04, S. und Marper gegen Großbritannien; und EGMR, 20. Januar 2010, Antrag Nr. 20689/08, W. gegen die Niederlande.

Zusammenfassung und Schlussfolgerungen

Die Datenschutzrichtlinie sieht eine Reihe von Rechten für natürliche Personen vor, wie das Recht, Auskunft über die eigenen Daten zu erhalten, diese zu sperren oder zu löschen, sowie das Recht, Informationen darüber zu verlangen, zu welchem Zweck und durch wen diese Daten verarbeitet werden. Sie sieht ebenfalls Rechtsmittel und Kompensation für erlittene Schäden vor. Diese Rechte sind jedoch allgemein formuliert und die Wege, über die diese ausgeübt werden können, werden nicht näher ausgeführt. Darüber hinaus variieren die Rechte in den verschiedenen Mitgliedstaaten – wie die Europäische Kommission in ihrer Folgenabschätzung feststellte⁵⁶ – aufgrund von Fragmentierung und inkonsequenter Um- und Durchsetzung. Des Weiteren sind sich die Betroffenen oftmals weder darüber bewusst, was mit ihren personenbezogenen Daten passiert, noch haben sie die Kontrolle hierüber, sodass die Ausübung ihrer Rechte im Grunde scheitert. Dies hat zu Vorschlägen für einen neuen EU-Rechtsrahmen im Datenschutz geführt.

In Hinsicht auf den Datenschutz der Betroffenen von Menschenhandel ist festzustellen, dass die Richtlinie sowohl für den öffentlichen als auch den privaten Sektor gilt, einschließlich internationaler und zwischenstaatlicher Organisationen, NROs und (kommerzieller) Unternehmen.

Von besonderer Relevanz ist das mögliche Argument, dass die Daten der Betroffenen von Menschenhandel für die Prostitution als „sensible Daten“ zu handhaben sind und somit strengeren Regeln unterliegen. Dies hat Auswirkungen auf ihre Erhebung, Speicherung und den Austausch der Daten der Betroffenen von Menschenhandel ohne deren informierte und freiwillig erfolgte Einwilligung,⁵⁷ beispielsweise im Rahmen internationaler Verweise.

⁵⁶ European Commission Impact Assessment, Anhang 2, Seite 21.

⁵⁷ Andere als die im Rahmen der Zusammenarbeit von Polizei und Gerichten in Strafsachen.

Die Datenschutzkonvention des Europarats (Konvention 108)

Übersicht über relevante Bestimmungen

Der Europarat nahm die Konvention 108 (eigentlich: „Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten“) 1981 an. Damals war sie das erste rechtlich bindende internationale Instrument für den Datenschutz. Nach Artikel 1 bestand ihre Aufgabe darin,

- » im Hoheitsgebiet [...] für jedermann [...] sicherzustellen, daß seine Rechte und Grundfreiheiten, insbesondere sein Recht auf einen Persönlichkeitsbereich, bei der automatischen Verarbeitung personenbezogener Daten geschützt werden.

Die Konvention setzt Mindeststandards für den Schutz personenbezogener Daten vor Missbrauch und reguliert den grenzüberschreitenden Transfer dieser Daten. Nach Artikel 11 können die Vertragsparteien auf Landesebene jeweils striktere Standards festlegen.⁵⁸

Derzeit haben 44 Mitgliedstaaten des Europarats die Konvention ratifiziert, darunter auch alle EU-Mitgliedstaaten.⁵⁹ Da die Konvention auch Nicht-Mitgliedern des Europarats offen steht, werden in Zukunft wohl noch weitere Drittstaaten die Konvention ratifizieren.

2012 haben der Europarat und der Beratende Ausschuss der Konvention einen Prozess zur Aktualisierung dieses Rechtsinstruments angestoßen. Primär verfolgen sie dabei zwei Ziele:

58 Nach Paragraph 48 des erläuternden Berichts zur Konvention 108 können die Vertragsparteien der Konvention höhere Standards für weitere Kategorien von Daten festlegen: „Der Grad der Sensitivität von Datenarten hängt vom rechtlichen und soziologischen Gefüge des betreffenden Staates ab.“ <http://conventions.coe.int/Treaty/en/Reports/Html/108.htm> .

59 Stand 8. März 2013. Eine Übersicht der Mitgliedstaaten findet sich hier: <http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?CL=GER&CM=&NT=108&DF=&VL=> .

- den veränderten Anforderungen an den Schutz der Privatsphäre angesichts der Nutzung neuer Informations- und Kommunikationstechnik (IKT) gerecht zu werden;
- den Kontrollmechanismus der Konvention zu stärken.

Geltungsbereich

Die Konvention 108 entstand lange vor der EU- Datenschutzrichtlinie, weshalb zu erwarten wäre, dass beide Verträge einen ähnlichen Schwerpunkt und Geltungsbereich haben. Dennoch bestehen zwischen beiden Texten einige wesentliche Unterschiede.

Bis heute ist die Konvention im Bereich Datenschutz das einzig bindende internationale Rechtsinstrument mit einem potenziell *weltweiten* Geltungsbereich, das prinzipiell allen Ländern offensteht, auch solchen, die nicht Mitglieder des Europarats sind. In der Praxis sind die meisten Vertragsparteien der Konvention auch Mitgliedstaaten der Europäischen Union.

Die Konvention zielt auf den Schutz der Privatsphäre – online wie offline – vor dem Zugriff durch Behörden und private Unternehmen. Anders als die Datenschutzrichtlinie findet sie auch in Bereichen wie Verteidigung, nationale Sicherheit und Polizei Anwendung.

Festzuhalten bleibt, dass die Konvention 108 bei der Definition von „automatischer Verarbeitung“ die Erhebung von Daten außen vor lässt. Die einzige Bestimmung, die sich auf die Erhebung personenbezogener Daten anwenden lässt, ist Artikel 5(e). Automatisch verarbeitete personenbezogene Daten, heißt es dort, müssen „nach Treu und Glauben und auf rechtmäßige Weise beschafft sein und verarbeitet werden“ und „müssen den Zwecken, für die sie gespeichert sind, entsprechen, dafür erheblich sein und dürfen nicht darüber hinausgehen“ und müssen „sachlich richtig“ sein.

Prinzipien und Bedingungen für die Datenverarbeitung

Für die Qualität der Daten ist Artikel 5 die zentrale Bestimmung und damit ähnlich zu Artikel 6 der Datenschutzrichtlinie, allerdings ist der Geltungsbereich von Artikel 5 enger gesteckt.

Konvention 108, Artikel 5 – Qualität der Daten

Personenbezogene Daten, die automatisch verarbeitet werden:

- a) müssen nach Treu und Glauben und auf rechtmäßige Weise beschafft sein und verarbeitet werden;
- b) müssen für festgelegte und rechtmäßige Zwecke gespeichert sein und dürfen nicht so verwendet werden, daß es mit diesen Zwecken unvereinbar ist;
- c) müssen den Zwecken, für die sie gespeichert sind, entsprechen, dafür erheblich sein und dürfen nicht darüber hinausgehen
- d) müssen sachlich richtig und wenn nötig auf den neuesten Stand gebracht sein;
- e) müssen so aufbewahrt werden, daß der Betroffene nicht länger identifiziert werden kann, als es die Zwecke, für die sie gespeichert sind, erfordern.

Artikel 9(2) sieht jedoch weitreichende Ausnahmeregelungen vor. Eine Abweichung von den Artikeln 5 (Qualität von Daten), 6 (besondere Arten von Daten) und 8 (zusätzlicher Schutz für den Betroffenen) ist für Mitgliedstaaten hiernach zulässig,

- » wenn sie durch das Recht der Vertragspartei vorgesehen und in einer demokratischen Gesellschaft eine notwendige Maßnahme ist:
 - a) zum Schutz der Sicherheit des Staates, der öffentlichen Sicherheit sowie der Währungsinteressen des Staates oder zur Bekämpfung von Straftaten;
 - b) zum Schutz des Betroffenen oder der Rechte und Freiheiten Dritter“.

Sensible Daten

Ähnlich der Datenschutzrichtlinie enthält die Konvention 108 spezifische Bestimmungen zur Verarbeitung sensibler Daten. In Artikel 6 (Besondere Arten von Daten) heißt es hierzu:

- » Personenbezogene Daten, welche die rassische Herkunft, politische Anschauungen oder religiöse oder andere Überzeugungen erkennen lassen, sowie personenbezogene Daten, welche die Gesundheit oder das Sexualleben betreffen, dürfen nur automatisch verarbeitet werden, wenn das innerstaatliche Recht einen geeigneten Schutz gewährleistet. Dasselbe gilt für personenbezogene Daten über Strafurteile.

Bis auf die Kategorien ethnische Herkunft, philosophische Überzeugungen, Mitgliedschaft in einer Gewerkschaft und Daten bezüglich Verurteilungen findet sie auf die gleiche Art von Daten wie Artikel 8 der EU-Datenschutzrichtlinie Anwendung.

Die Konvention beschreibt weder die verschiedenen Kategorien der besonderen Arten von Daten näher noch gibt sie Angaben darüber, was „geeigneter Schutz“ wäre. Daher lässt den Vertragsparteien einen weiten Ermessensspielraum.

Die in Artikel 9(2) beschriebenen Ausnahmen finden auch auf sensible Daten Anwendung.

Sanktionen

Die Konvention verlangt die Umsetzung ihrer Prinzipien in nationale Gesetze und die Festlegung entsprechender Sanktionen und Rechtsmittel für eine Verletzung ihrer Vorschriften (Artikel 10). Sanktionen und Rechtsmittel können sowohl zivil-, verwaltungs- als auch strafrechtlicher Natur sein und hängen allein von den Gegebenheiten im jeweiligen Land ab.

Es gibt keine Vorgabe zur Einrichtung weiterer Mechanismen wie einer Kontrollstelle und die Konvention verpflichtet die Vertragsparteien auch nicht zum Aufbau institutionalisierter Mechanismen zur unabhängigen Untersuchung von Beschwerden. Zur Behebung dieser Schwächen trat zum 1. Juli 2004 ein Zusatzprotokoll in Kraft, das die Vertragsparteien zur Einrichtung einer Kontrollstelle verpflichtet, die ihre Aufgaben in vollständiger Unabhängigkeit wahrnimmt und so zu einem wirksamen Schutz einzelner Personen beiträgt.⁶⁰

⁶⁰ Zusatzprotokoll zum Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten bezüglich Kontrollstellen und grenzüberschreitendem Datenverkehr (SEV Nr. 181).

3. DAS KONZEPT „SENSIBLER DATEN“ UND DIE VERPFLICHTENDE REGISTRIERUNG VON SEXARBEITER*INNEN ALS MITTEL ZUR BEKÄMPFUNG DES MENSCHENHANDELS⁶¹

In diesem Kapitel wird ein konkretes Beispiel für die Anwendung des Konzepts der „sensiblen Daten“ anhand des Falls der verpflichtenden Registrierung von Sexarbeiter*innen in den Niederlanden erörtert.

2009 wurde dem Parlament der Niederlande ein Gesetz zur Bekämpfung des Menschenhandels vorgelegt, welches die verpflichtende Registrierung von Sexarbeiter*innen und die Kriminalisierung nicht-registrierter Sexarbeiter*innen und ihrer Kund*innen vorsah.

Zentrales Ziel dieses Gesetzesvorschlags war die Verbesserung der Kontrolle und die Durchsetzung der Gesetze in der Sexindustrie. Eine verpflichtende Registrierung, so wurde argumentiert, diene der Bekämpfung des Menschenhandels und anderer Formen des Missbrauchs in der Sexindustrie, da fortan klar wäre, wer die Prostituierten seien und wo diese arbeiteten. Außerdem würde die Registrierung „die Chance zu einem Kontakt“ mit Sexarbeiter*innen und die Möglichkeit zur Identifizierung von zwangsweise prostituierten Personen bieten sowie die Aufklärung von Sexarbeiter*innen über ihre Rechte und die Unterbreitung von Unterstützungsangeboten ermöglichen.

Das Gesetz traf auf den erbitterten Widerstand von Sexarbeiter*innen, NROs, Expert*innen, Akademiker*innen und anderen Personen, die zu Sexarbeit und Menschenhandel arbeiten. Nicht nur glaubte fast niemand, dass eine verpflichtende Registrierung der Bekämpfung des Menschenhandels dienen würde, es war auch klar, dass eine nationale Datenbank zu Sexarbeiter*innen datenschutzrechtlich sehr sensibel war.

⁶¹ Dieses Kapitel beruht auf einer von der Dutch Association of Women and Law bei Van der Feltz advocaten (W.I. Koelewijn & R.L. de Graaff) in Auftrag gegebenen Untersuchung der rechtlichen Vereinbarkeit des Gesetzes aus dem Jahr 2009 zur verpflichtenden Registrierung von Sexarbeiter*innen mit der Datenschutzrichtlinie und den entsprechenden Bestimmungen im niederländischen Gesetz.

Dies führte zu der Frage, ob die verpflichtende Registrierung von Sexarbeiter*innen unter das Verbot zur Sammlung von Daten zum Sexualleben einer Person (Artikel 8 der Datenschutzrichtlinie und Artikel 16 des niederländischen Gesetzes zum Schutz personenbezogener Daten Wbp⁶²) fallen würde.

Nach Einschätzung des niederländischen Staatsrates⁶³ war dies der Fall und die Registrierung hätte somit strikten Kriterien unterlegen. Es hätten ein besonderes öffentliches Interesse festgestellt und ausreichend Sicherheiten für den Schutz des Persönlichkeitsbereichs sichergestellt und eine rechtliche Grundlage geschaffen werden müssen. Nach Ansicht des Staatsrats stand das Interesse der Stärkung von Kontrolle und der Durchsetzung von Gesetzen nicht im Verhältnis zu den zur Erreichung der Ziele vorgeschlagenen Mitteln, in diesem Fall die verpflichtende Registrierung aller Sexarbeiter*innen. Folglich ging der Staatsrat davon aus, dass das Gesetz weder die „Notwendigkeitsprüfung“ bestehen konnte, noch das Kriterium eines besonderen öffentlichen Interesses erfüllte.

Der niederländische Innenminister ignorierte jedoch die Kritik des Staatsrats und argumentierte, dass das in Artikel 23 Wbp (Artikel 8 der Datenschutzrichtlinie) enthaltene Verbot nicht anwendbar war, da Sexarbeit seiner Meinung nach eben als Arbeit anzusehen war. Daraus folgerte er, dass Daten zur Sexarbeit nicht als Daten zum Sexualleben einer Person betrachtet werden konnten, da sie sich auf das berufliche und nicht auf das private (Sexual)leben, die sexuellen Vorlieben oder sexuelle Orientierung einer Person bezogen.

Damit rückte die Definition von „Sexualleben“ in den Fokus sowie die Frage, ob sich eine Unterscheidung zwischen dem privaten und beruflichen Sexualleben einer Person rechtfertigen ließ.

⁶² Wet bescherming persoonsgegevens (Wbp). Die Wbp ist die niederländische Umsetzung der Datenschutzrichtlinie. Ihre Bestimmungen sollten daher in Einklang mit der Datenschutzrichtlinie interpretiert werden.

⁶³ Raad van State, No.W04.09.01 50/1, 11. September 2009. Der Staatsrat berät die Regierung.

Wie bereits erwähnt, wird „Sexualleben“ weder in der Datenschutzrichtlinie noch in ihrer Präambel definiert oder erklärt. Auch die Rechtsprechung des Europäischen Gerichtshofs bietet keine Interpretation des Konzepts „Sexualleben“. Jedoch hat der Europäische Gerichtshof für Menschenrechte (EGMR) in mehreren Fällen entschieden, dass die Sexualität zu den intimsten Aspekten des Persönlichkeitsbereichs einer Person gehört und dass eine Einmischung der Regierung in diesen Bereich in einer demokratischen Gesellschaft besonders schwerwiegender Gründe bedarf.⁶⁴

Darüber hinaus wird die Unterscheidung zwischen dem beruflichen und dem privaten Leben einer Person weder von der Rechtsprechung des EuGH noch des EGMR unterstützt. Hier beruft sich der EuGH auf den EGMR, der in mehreren Fällen entschieden hat, dass „der Begriff ‚Privatleben‘ nicht eng interpretiert werden darf“ und dass „es keinen prinzipiellen Grund gibt, mit der sich der Ausschluss einer beruflichen oder unternehmerischen Aktivität aus dem Rahmen des rein ‚privaten‘ rechtfertigen lässt“.⁶⁵ Insbesondere gilt dies bei freiberuflichen Tätigkeiten, bei denen die „berufliche und nicht-berufliche Tätigkeit so eng verwoben [ist], dass eine Unterscheidung zwischen beiden fast unmöglich [scheint]“.⁶⁶ Bestätigt wurde dies im Fall *Khelili gegen die Schweiz*.⁶⁷

Zudem hatte zum Zeitpunkt der Umsetzung des niederländischen Gesetzes zum Schutz personenbezogener Daten der damalige Justizminister auf die Frage, ob das Konzept „Sexualleben“ beispielsweise auch für eine promiske Sexualität gelte, geantwortet:

- » Promiskuität oder die Frage, ob sich Menschen regelmäßig im Rotlichtbezirk aufhalten, fällt unter Sexualleben. Dies ist somit etwas anderes als die sexuelle Orientierung.

64 EGMR, 22. Oktober 1981, Entscheidung Nr. 7525/76, *Dudgeon gegen das Vereinigte Königreich*; EGMR, 26. Oktober 1988, Entscheidung Nr. 10581/83, *Norris gegen Irland*.

65 EuGH, C-92/09 und C93/09 vom 9. November 2010, *Schecke & Eifert*, § 59. Siehe auch EuGH, C-456/00, *Österreichischer Rundfunk und andere*, §§ 73 und 74; EuGH, 8. November 2007, T-194/04, *Bavarian Lager Co. Ltd.*; und EGMR 16. Dezember 1992, Entscheidung Nr. 13710/88, *Niemitz gegen Bundesrepublik Deutschland*, § 29.

66 EGMR, 16. Dezember 1992, Entscheidung Nr. 13710/88, *Niemitz gegen Bundesrepublik Deutschland*, § 29.

67 EGMR, 18. Oktober 2011, Entscheidung Nr. 16188/07, *Khelili gegen die Schweiz*, § 56.

Nur schwer ließ sich der Standpunkt aufrechterhalten, dass Daten zur Frequentierung von Sexarbeiter*in sensibel seien, während dies für die Tatsache, Sexarbeiter*in zu sein, nicht gelten sollte. Gleichfalls folgte aus der niederländischen Rechtsprechung, dass die Kategorisierung von Daten als „sensibel“ nicht von den mit der Datenverarbeitung verfolgten Zielen abhing, sondern einzig und allein von der Natur der Daten.⁶⁸

Daraus folgte, dass die Unterscheidung, die der Minister zwischen dem beruflichen und dem privaten Sexualleben gemacht hatte, weder vor dem EuGH noch vor dem EGMR Bestand haben konnte. Somit musste der Justizminister zugeben, dass sich eine Unterscheidung zwischen dem beruflichen und dem privaten Sexualleben von Sexarbeiter*innen nicht aufrechterhalten ließ und dass, entgegen seiner früheren Äußerungen, die Registrierung von Sexarbeiter*innen durchaus die Verarbeitung sensibler Daten betraf.

Daher wurde die Registrierung von Sexarbeiter*innen nach Artikel 16 des niederländischen Datenschutzgesetzes (Wbp), der niederländischen Umsetzung der Datenschutzrichtlinie, verboten. Als Nächstes stellte sich folglich die Frage, ob die Bedingungen für eine Ausnahme zu diesem Verbot gegeben waren.

Nach Artikel 23 (1) f des niederländischen Datenschutzgesetzes (entspricht Artikel 8 der Datenschutzrichtlinie) ist eine Ausnahme zum allgemeinen Verbot einer Verarbeitung sensibler Daten nur unter strikten Bedingungen zu genehmigen. Entsprechend der Datenschutzrichtlinie hätten ein besonderes öffentliches Interesse festgestellt und ausreichende Garantien für den Schutz des Persönlichkeitsbereichs gegeben sowie eine rechtliche Grundlage geschaffen werden müssen.⁶⁹

Nach niederländischer Rechtsprechung muss die Frage, ob es ein für die Verarbeitung sensibler Daten legitimes Ziel gibt oder nicht, im Licht der Art, Schwere und des Ausmaßes des Problems betrachtet werden,

⁶⁸ Hoge Raad, 23. März 2010, LJN BK6331.

⁶⁹ Entweder durch nationale Gesetze oder per Entscheidung der Kontrollstelle.

das diese Verarbeitung lösen soll.⁷⁰ Besteht tatsächlich ein bedeutendes öffentliches Interesse, muss entsprechend abgewogen werden, ob die Verarbeitung sensibler Daten im Rahmen dieses Interesses auch *notwendig* ist. Im Kontext dieser „Notwendigkeitsprüfung“ folgt aus europäischer Rechtsprechung, dass die Mittel (sprich die Verarbeitung sensibler Daten) zur Erreichung des Ziels geeignet und verhältnismäßig sein sollten und dass es keine weniger schwerwiegenden Mittel geben sollte, mit denen sich das gleiche Ziel erreichen ließe.

Für eine Bewertung, ob sich eine Ausnahme aus „Gründen eines bedeutenden öffentlichen Interesses“ rechtfertigen lässt, musste man sich die Zielsetzung des Gesetzes anschauen. Trotz der Beteuerungen, den Menschenhandel bekämpfen zu wollen, verfolgte das Gesetz eigentlich nur das Ziel einer Regulierung der „Prostitution und der Sexindustrie“ und einer „Erleichterung der Kontrolle und Durchsetzung der Gesetze“. Es war sehr zweifelhaft, ob gerade dieses Ziel, vor allem unter dem Gesichtspunkt der Verhältnismäßigkeit, einen schwerwiegenden Eingriff in das Recht aller Sexarbeiter*innen in den Niederlanden auf Schutz der Privatsphäre rechtfertigte. In diesem Sinne fehlte dem Gesetz auch eine Motivation hinsichtlich Art, Schwere und Ausmaß von Misshandlungen in der Sexindustrie, die, aus Sicht des Gesetzes, ein derart schwerwiegendes öffentliches Interesse begründet hätten, um einen solchen Eingriff zu rechtfertigen. Zudem bestanden wesentlich effektivere Mittel, die einen sehr viel kleineren Eingriff in den Persönlichkeitsbereich von Sexarbeiter*innen bedeutet hätten. Beispielsweise hätte die Kontrolle von Bordellen und nicht die Überwachung einzelner Sexarbeiter*innen ausgeweitet werden können. Genauso hätten Beratungsangebote für Sexarbeiter*innen ausgebaut werden können, um sie mit Information und Unterstützung zu versorgen.

In diesem Zusammenhang war es auch wichtig, dass eine große Anzahl von NROs, Expert*innen und Jurist*innen ihre Bedenken öffentlich machten, dass eine verpflichtende Registrierung zu einer umgekehrten Reaktion führen und Menschen in die Illegalität treiben könnte und viele Sexarbeiter*innen

70 Siehe beispielsweise ABRvS 3. September 2008, LJN BE9698.

dann nicht mehr für Fachberatungsstellen und Mitarbeiter*innen des Gesundheitssystems erreichbar wären. Auch die Abschließenden Bemerkungen (Concluding Observations) des CEDAW-Ausschusses für die Niederlande 2010 gaben dieser Sorge Raum:

- » 30. Sorge bereitet dem Ausschuss, dass das neue Prostitutionsgesetz der Niederlande zur verpflichtenden Registrierung von Prostituierten die Mehrheit der Prostituierten in die Illegalität treiben könnte. Unter diesen Prostituierten befinden sich viele Migrant*innen aus Drittländern, die keine Möglichkeit zur Registrierung haben. Daher befürchtet der Ausschuss, dass das Gesetz die Situation von Prostituierten nicht verbessern wird, sondern ganz im Gegenteil die Bemühungen zur Bekämpfung der sexuellen Ausbeutung von Frauen durchkreuzen und die Verwundbarkeit von Prostituierten erhöhen könnte, die sich entweder nicht registrieren lassen können oder wollen, in dem es ihre Arbeitsbedingungen verschlechtert und ihre soziale Ausgrenzung verschärft. Es steht zu befürchten, dass dieses neue Gesetz für den Persönlichkeitsbereich und die Sicherheit registrierter Prostituierter ernsthafte Risiken birgt.
- 31. Der Ausschuss mahnt den Vertragsstaat zu einer sorgfältigen Analyse der Risiken des neuen Gesetzes, auch unter dem Gesichtspunkt der Wahrung des Persönlichkeitsbereichs. Vor der Verabschiedung des Gesetzes sollte es Gespräche mit entsprechenden Gruppen und relevanten Organisationen geben. Weiterhin ruft der Ausschuss die Niederlande dazu auf, in ihrem nächsten periodischen Bericht umfassendere und konkretere Informationen zu Maßnahmen zur Verbesserung der Arbeitsbedingungen von Prostituierten und zur Stärkung ihrer Autonomie, des Schutzes ihres Persönlichkeitsbereichs und ihrer Sicherheit vorzulegen.⁷¹

⁷¹ Siehe Concluding Observation of the Committee on the Elimination of Discrimination against Women, Seite 7 und 8 einzusehen unter: <http://www2.ohchr.org/english/bodies/cedaw/docs/co/CEDAW-C-NLD-CO-5.pdf>.

Neben der Bedingung eines bedeutenden öffentlichen Interesses müssen auch geeignete Maßnahmen zum Schutz der Privatsphäre getroffen werden. Dabei muss bedacht werden, dass der EGMR bei der Verarbeitung sensibler Daten höhere Standards in Bezug auf die Sicherheitsstufe, den Speicherzeitraum der Daten, die Zugriffsmöglichkeiten und die (rechtlich, per Gesetz) festgelegten Garantien zum Schutz des Persönlichkeitsbereichs setzt.⁷²

Würden die Registrierungsdaten schließlich der Polizei zugänglich gemacht, unterläge ihre Verarbeitung dem Polizeigesetz. So wäre es denkbar, dass Daten über Prostituierte, die sowohl nach dem Datenschutzgesetz als auch laut des vorgeschlagenen Gesetzes nicht in der zentralen Datenbank gespeichert werden sollten, in der Polizeidatenbank lägen. Für die Speicherdauer und die Verarbeitung von Daten gelten bei der Polizei andere Regeln. Zudem erlaubt das Polizeigesetz den Austausch von Daten zwischen verschiedenen Einheiten der Polizei, der Polizei und Dritten sowie zwischen der niederländischen Polizei und der Polizei anderer Länder. Der letztgenannte Austausch könnte die Risiken für Migrant*innen bei der Rückkehr in ihre Herkunftsländer erhöhen, insbesondere in Fällen, in denen das dortige nationale Recht Sexarbeit kriminalisiert.

Aufgrund schwerwiegender Einwände der ersten niederländischen Parlamentskammer (dem Senat) gegen die verpflichtende Registrierung von Prostituierten sah sich der Minister im Juli 2013 zur Rücknahme seines Gesetzesentwurfs gezwungen.

⁷² Siehe z. B. EGMR, 4. Dezember 2008, Entscheidung Nr. 30562/04 und 30566/04, S. und Marper gegen das Vereinigte Königreich; und EGMR, 20. Januar 2010, Entscheidung Nr. 20689/08, W. gegen die Niederlande.

4. SPEZIFISCHE DATENSCHUTZVORKEHRUNGEN IN RECHTSINSTRUMENTEN ZUR BEKÄMPFUNG DES MENSCHENHANDELS

In diesem Kapitel werden Vorkehrungen zum Datenschutz und zum Recht auf Privatsphäre in der europäischen Gesetzgebung zur Bekämpfung des Menschenhandels aufgezeigt sowie politische Instrumente und weitere „soft law“-Empfehlungen erläutert.

a. **Übereinkommen des Europarats zur Bekämpfung des Menschenhandels**

Nach dem Übereinkommen des Europarats zur Bekämpfung des Menschenhandels (CoE Trafficking Convention) hat die Nutzung der personenbezogenen Daten von Betroffenen von Menschenhandel in Einklang mit den Bestimmungen der Konvention 108 zu erfolgen und zwar unabhängig davon, ob die Mitgliedstaaten die Konvention ratifiziert haben oder nicht.⁷³

Artikel 11 der CoE Trafficking Convention enthält folgende Bestimmungen zum Schutz des Persönlichkeitsbereichs:

1. Jede Vertragspartei schützt das Privatleben und die Identität der Betroffenen. Personenbezogene Daten über die Betroffenen werden nach Maßgabe des Übereinkommens zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (SEV Nr. 108) gespeichert und verwendet.
2. Jede Vertragspartei trifft Maßnahmen, um insbesondere sicherzustellen, dass die Identität eines Kindes, das von Menschenhandel betroffen ist, oder Einzelheiten, welche die Identifizierung eines solchen Kindes ermöglichen, nicht durch die Medien oder auf sonstige Weise öffentlich

⁷³ Erläuternder Bericht zur Konvention des Europarates zur Bekämpfung des Menschenhandels, § 141 (auf Englisch): <http://www.conventions.coe.int/Treaty/EN/Reports/Html/197.htm> .

bekannt gemacht werden, es sei denn, um in Ausnahmefällen Familienmitglieder des Kindes ausfindig zu machen oder auf andere Weise sein Wohl und seinen Schutz zu gewährleisten.

3. Jede Vertragspartei erwägt in Übereinstimmung mit Artikel 10 der Konvention zum Schutz der Menschenrechte und Grundfreiheiten in der Auslegung durch den Europäischen Gerichtshof für Menschenrechte Maßnahmen mit dem Ziel, die Medien zu veranlassen, das Privatleben und die Identität der Betroffenen zu schützen, sei es durch Selbstregulierung oder durch regulierende Maßnahmen, die vom Staat allein oder vom Staat und dem Privatsektor gemeinsam getroffen werden.

Wie der Europarat in seinem ‚Erläuternden Bericht zur Konvention‘ (Explanatory Report of the Council of Europe Convention) feststellt, ist der Schutz des Privatlebens und der Identität der Betroffenen von Menschenhandel angesichts der von den Menschenhändler*innen ausgehenden Gefahr grundlegend für die physische Sicherheit der Betroffenen. Sie dient, auch angesichts von Scham und der Gefahr der Stigmatisierung sowohl der Betroffenen als auch von deren Familien, der Wahrung von Chancen auf soziale Integration im Herkunftsland, im Zielland oder in einem Drittland.⁷⁴

Auch Artikel 30 der Konvention bezieht sich auf den Persönlichkeitsbereich⁷⁵. Hier geht es konkret um den Schutz des Privatlebens und der Identität von Betroffenen von Menschenhandel im Rahmen von Gerichtsverfahren.

Artikel 11(2) fordert, besondere Maßnahmen gegen die Veröffentlichung der Identität eines Kindes bzw. von persönlichen Details, die die Identifizierung eines Kindes ermöglichen, zu treffen. Allerdings ist die Entscheidung über Maßnahmen zum Schutz der Identität bzw. von persönlichen Details,

74 Erläuternder Bericht zur Konvention des Europarates zur Bekämpfung des Menschenhandels, § 138.

75 Artikel 30 - Gerichtsverfahren: In Übereinstimmung mit der Konvention zum Schutz der Menschenrechte und Grundfreiheiten, insbesondere Artikel 6, trifft jede Vertragspartei nach Maßgabe ihres internen Rechts und im Fall von Opfern, die Kinder sind, unter besonderer Berücksichtigung der Bedürfnisse von Kindern und unter Gewährleistung ihres Anspruchs auf besondere Schutzmaßnahmen die erforderlichen gesetzgeberischen oder anderen Maßnahmen, um während gerichtlicher Verfahren a) den Schutz des Privatlebens und erforderlichenfalls der Identität der Opfer; b) die Sicherheit der Opfer und deren Schutz vor Einschüchterung zu gewährleisten.

die die Identifizierung von vom Menschenhandel betroffenen Kindern ermöglichen würden, alleine Sache der jeweiligen Vertragspartei. Hierzu bestehen in einigen Ländern Gesetze, die Strafen für die Veröffentlichung von Informationen vorsehen, anhand derer sich die Betroffenen bestimmter Straftaten identifizieren lassen.⁷⁶

Dennoch erlaubt Paragraph 2 in Ausnahmefällen die Veröffentlichung von Informationen bezüglich der Identität von minderjährigen Betroffenen von Menschenhandel, sollte dies zum Auffinden von Verwandten oder auf andere Weise der Gewährleistung des Wohls und Schutzes des Kindes dienen.

Schließlich bestimmt Artikel 11 (3), dass die Vertragsparteien Maßnahmen mit dem Ziel zu treffen haben, die Medien zu veranlassen, das Privatleben und die Identität der Betroffenen zu schützen. Um nicht mit dem Gut der Pressefreiheit zu kollidieren, argumentiert Paragraph 3, dass solche Maßnahmen in Übereinstimmung mit Artikel 10 der Konvention zum Schutz der Menschenrechte stehen müssen und ausschließlich dem Schutz des Privatlebens und der Identität der Betroffenen dienen müssen.

b. UN-Zusatzprotokoll zur Verhütung, Bekämpfung und Bestrafung des Menschenhandels, insbesondere des Frauen- und Kinderhandels

Das Zusatzprotokoll zur Verhütung, Bekämpfung und Bestrafung des Menschenhandels, insbesondere des Frauen- und Kinderhandels zum Übereinkommen der Vereinten Nationen gegen die grenzüberschreitende organisierte Kriminalität (im Folgenden „UN-Menschenhandelsprotokoll“), ist das erste weltweit bindende Rechtsinstrument, welches eine allgemeine Definition des Menschenhandels enthält.

⁷⁶ Erläuternder Bericht zur Konvention des Europarates zur Bekämpfung des Menschenhandels, § 143.

Zum Schutz oder zur Verarbeitung von Daten enthält das Menschenhandelsprotokoll jedoch keine Bestimmungen. Lediglich Artikel 10 erwähnt, dass die

- » Strafverfolgungs-, Einwanderungs- oder sonstigen zuständigen Behörden der Vertragsstaaten [...] gegebenenfalls miteinander zusammen[arbeiten], indem sie in Übereinstimmung mit ihrem innerstaatlichen Recht Informationen austauschen [...].

c. Richtlinie 2011/36/EU des europäischen Parlaments und des Rates vom 5. April 2011 zur Verhütung und Bekämpfung des Menschenhandels und zum Schutz seiner Opfer

Richtlinie 2011/36/EU vom 5. April 2011 zur Verhütung und Bekämpfung des Menschenhandels und zum Schutz seiner Opfer (im Folgenden „Menschenhandelsrichtlinie“) bietet bindende Gesetzesvorschriften zur Bekämpfung des Menschenhandels, zur effektiven Bestrafung der Täter*innen und zum besseren Schutz der Betroffenen.

Erwägung 33 der Präambel der Richtlinie bestätigt die Achtung der fundamentalen Rechte und die Einhaltung der Prinzipien,

- » die insbesondere mit der Charta der Grundrechte der Europäischen Union anerkannt wurden; dazu gehören vor allem [...] der Schutz personenbezogener Daten [...]. Diese Richtlinie, die insbesondere darauf abzielt, die uneingeschränkte Wahrung dieser Rechte und Grundsätze zu gewährleisten, ist entsprechend umzusetzen.

5. HERAUSFORDERUNGEN AN DEN DATENSCHUTZ IN DEN RICHTLINIEN ZUR BEKÄMPFUNG DES MENSCHENHANDELS

Im folgenden Kapitel werden die Anwendungen des Datenschutzrechts und der Maßnahmen zur Bekämpfung des Menschenhandels im Hinblick auf ihre praktische Umsetzung diskutiert. Des Weiteren werden Empfehlungen für Akteure zur Bekämpfung des Menschenhandels mit dem Schwerpunkt auf NROs ausgesprochen.

Übersicht

Nationale Berichterstattungsstellen und andere Datenerhebungsinstrumente	
Herausforderungen	<ul style="list-style-type: none">• Die Erhebung von Daten zu vom Menschenhandel betroffenen Personen kann auch die Erhebung personenbezogener Daten bedeuten
datACT-Empfehlungen	<ul style="list-style-type: none">• Standards für die Zusammenarbeit mit NROs festlegen• Eintreten für die Nutzung ausschließlich anonymisierter Daten
Identifizierung von vom Menschenhandel Betroffener und Zugang zu Unterstützungsstrukturen	
Herausforderungen	<ul style="list-style-type: none">• Registrierung und Übertragung der personenbezogenen Daten von Betroffenen zwischen Herkunfts- und Zielland und zwischen den Behörden auf Landesebene
datACT-Empfehlungen	<ul style="list-style-type: none">• Durchführung sogenannter Privacy Impact Assessments (PIA)• Weitestmögliche Vermeidung der Weitergabe personenbezogener Daten• Aufrechterhaltung und Forderung nach einem dezentralisierten anonymen Zugang zu Unterstützungsstrukturen für Betroffene von Menschenhandel

Nicht-staatliche Fachberatungsstellen zur Bekämpfung des Menschenhandels

Herausforderungen	<ul style="list-style-type: none">• Die interne computergestützte Dokumentation von Fällen und das System zur Verwaltung dieser Daten ist evtl. nicht sicher• NRO-Berater*innen sind evtl. gezwungen, die personenbezogenen Daten von Betroffenen mit Polizei- und Justizbeamten zu teilen• Die Rechte Betroffener von Menschenhandel als Datensubjekte sind möglicherweise nicht Teil des Beratungsangebots
datACT-Empfehlungen	<ul style="list-style-type: none">• Etablierung sicherer PIA-basierter IT Soft- und Hardware in Fachberatungsstellen für Betroffene von Menschenhandel• Eintreten für einen sorgfältigeren Umgang mit der Vertraulichkeitsverpflichtung und dem Recht zur Aussageverweigerung vor Gericht für Betroffene von Menschenhandel• Einführung von Beratungsmodulen zum Recht auf Schutz der Privatsphäre

5.1 Nationale Berichterstattungsstellen (NREM) und andere Instrumente zur Datenerhebung



Herausforderungen: Die Erhebung von Daten zu vom Menschenhandel Betroffener kann auch die Erhebung personenbezogener Daten bedeuten.

datACT-Empfehlungen:

- > Standards festsetzen für die Zusammenarbeit von NROs mit nationalen Berichterstattungsstellen und/oder einem gleichwertigen Mechanismus
- > Forderung nach Weitergabe ausschließlich anonymisierter Daten

Für ein besseres Verständnis der Trends und des Umfangs des Menschenhandels entstanden während der letzten Jahre sowohl auf globaler wie auch auf nationaler Ebene einzelner Länder verschiedene Datenerhebungsverfahren.

Entwickelt wurde die Idee eines systematischen und koordinierten Mechanismus zur Datenerhebung über den Menschenhandel in Artikel III.1.4 der Haager Ministererklärung vom 26. April 1997:

- » Einsetzung bzw. Auslotung der Möglichkeiten zur Einsetzung nationaler Berichterstatter, die den Regierungen über das Ausmaß, Präventionsmaßnahmen und die Bekämpfung des Frauenhandels Bericht erstatten. Diese sollten Kriterien entwickeln, die Aussagen über das Ausmaß, die Formen und die Funktionsweise des Frauenhandels und die Wirksamkeit von Richtlinien und Maßnahmen zur Bekämpfung dieser Phänomene erlauben. Die regelmäßige Zusammenarbeit zwischen den nationalen Berichterstattern sollte gefördert werden.⁷⁷

Für die meisten rechtlichen und politischen Instrumente zur Bekämpfung des Menschenhandels in Europa und der Mitgliedstaaten der OSZE (Organisation für Sicherheit und Zusammenarbeit in Europa), der EU und des Europarats blieb es zwar für mehr als ein Jahrzehnt nur ein optionaler Mechanismus, 2011 wurde die Berufung von nationalen Berichterstattungsstellen bzw. die Entwicklung eines gleichwertigen Mechanismus jedoch für alle EU-Mitgliedstaaten verpflichtend.

Artikel 19 der Richtlinie 2011/36 EU verpflichtet die Mitgliedstaaten, alle erforderlichen Maßnahmen zur Einsetzung nationaler Berichterstattungsstellen oder eines gleichwertigen Mechanismus zu treffen.⁷⁸ Regierungen sind zur Sammlung der notwendigen Daten aufgefordert zu einer engen Zusammenarbeit mit Organisationen der Zivilgesellschaft:

- » Die Mitgliedstaaten treffen die erforderlichen Maßnahmen, um nationale Berichterstatter einzusetzen oder gleichwertige Mechanismen einzuführen. Diese Mechanismen haben unter anderem die Aufgabe, die Entwicklungen beim Menschenhandel zu bewerten, die Ergebnisse der Maßnahmen zur

77 Haager Ministererklärung vom 26. April 1997 zu europäischen Leitlinien für wirksame Maßnahmen zur Verhütung und Bekämpfung von Frauenhandel mit dem Ziel der sexuellen Ausbeutung. Ministerkonferenz unter der Präsidentschaft der EU, Den Haag, 24.-26. April 1997. www.legislationline.org.

78 Richtlinie 2011/36/EU des Europäischen Parlaments und des Rates vom 5. April 2011 zur Verhütung und Bekämpfung des Menschenhandels und zum Schutz seiner Opfer sowie zur Ersetzung des Rahmenbeschlusses 2002/629/JI des Rates.

Bekämpfung des Menschenhandels zu messen, wozu auch die Sammlung statistischer Daten in enger Zusammenarbeit mit einschlägigen Organisationen der Zivilgesellschaft, die auf diesem Gebiet tätig sind, gehört, und Bericht zu erstatten. (Artikel 19)⁷⁹

In einem gemeinsamen Kommentar zur Richtlinie schreiben die UN-Agenturen, dass sämtliche Daten auf Grundlage allgemeiner Definitionen und eines gemeinsamen Verständnisses der Schlüsselkonzepte nach Geschlecht und Alter aufgeschlüsselt werden sollten und alle Formen des Menschenhandels abgedeckt werden sollten. Dies sollte geschehen

- » unter vollumfänglicher Wahrung des Schutzes des Persönlichkeitsbereichs von vom Menschenhandel Betroffenen und in Übereinstimmung mit der Richtlinie zum Schutz von Individuen in Bezug auf die Verarbeitung personenbezogener Daten und der freien Bewegung solcher Daten garantieren.⁸⁰

Politische Empfehlungen für europäische Systeme zur Datenerhebung

Während der letzten zehn Jahre entstanden zahlreiche Empfehlungen und Richtlinien sowie rechtliche Bestimmungen zur Einrichtung von Strukturen wie nationalen Berichterstattungsstellen und/oder gleichwertigen Mechanismen. In der Konvention des Europarats zur Bekämpfung des Menschenhandels von 2005 heißt es:

- » Jede Vertragspartei erwägt die Einsetzung nationaler Berichtersteller beziehungsweise Berichterstellerinnen oder andere Mechanismen für die Überwachung des Vorgehens der staat-

79 Richtlinie 2011/36/EU des Europäischen Parlaments und des Rates vom 5. April 2011 zur Verhütung und Bekämpfung des Menschenhandels und zum Schutz seiner Opfer sowie zur Ersetzung des Rahmenbeschlusses 2002/629/JI des Rates.

80 Prevent. Combat. Protect. Human Trafficking. Joint UN Commentary on the EU Directive – A Human Rights-Based Approach, November 2011, S. 100; http://www.unodc.org/documents/human-trafficking/2011/UN_Commentary_EU_Trafficking_Directive_2011.pdf.

lichen Institutionen bei der Bekämpfung des Menschenhandels und der Umsetzung der Erfordernisse in Bezug auf die innerstaatliche Gesetzgebung. (Artikel 29(4))

Das Übereinkommen fordert die Vertragsparteien auch zum Schutz des Privatlebens von Betroffenen auf (Artikel 11(1)3).

2006 veröffentlichte der Ministerrat der OSZE (MC.DEC/14/06, 5. Dezember 2006) die Stellungnahme „Verstärkung der Bemühungen zur Bekämpfung des Menschenhandels, einschließlich der Ausbeutung von Arbeitskräften, durch einen umfassenden und aktiven Ansatz“. Hierin drängt er die teilnehmenden Staaten

- » mit Unterstützung der OSZE-Organe und -Institutionen, wenn darum ersucht wird, die Forschung und das System zur Sammlung und Analyse von Daten unter gebührender Berücksichtigung des vertraulichen Charakters der Daten zu verbessern und die Statistiken wo immer möglich nach Geschlecht, Alter und gegebenenfalls anderen einschlägigen Faktoren zu gliedern, um Art und Umfang des Problems besser einschätzen und wirksame und zielgerichtete politische Maßnahmen gegen den Menschenhandel entwickeln zu können. Zu diesem Zweck wird den Teilnehmerstaaten empfohlen, die Bestellung nationaler Berichtserstatter oder ähnlicher unabhängiger Überwachungsmechanismen in Erwägung zu ziehen. (Artikel 3)⁸¹

Seit 2008 gibt die Alliance against Trafficking in Persons, ein informelles Netzwerk internationaler Organisationen und NROs, das sich regelmäßig unter der Schirmherrschaft der OSZE trifft, eine Stellungnahme zur Definition einer nationalen Berichterstattungsstelle und/oder gleichwertigen Mechanismus heraus (von dem *der Sonderbeauftragten und Koordinator* in der OSZE für die Bekämpfung des Menschenhandels am 16. Oktober 2008 im Namen

81 Beschluss Nr. 14/06 Verstärkung der Bemühungen zur Bekämpfung des Menschenhandels, einschließlich der Ausbeutung von Arbeitskräften, durch einen umfassenden und aktiven Ansatz. MC.DEC/14/06.

des Alliance Expert Coordination Teams (AECT) vorgelegt). Es beschreibt die Rolle der nationalen Berichterstattungsstelle auf detailliertere Weise:

- » Im Allgemeinen konzentrieren sich die Empfehlungen zu einem solchen Mechanismus auf
 1. die Identifizierung des Ausmaßes des Problems,
 2. der Förderung des Informationsaustauschs zwischen Partnern auf der internationalen Ebene,
 3. den Aufruf an den jeweils zuständigen Mechanismus zur Verfassung eines jährlichen Berichts zur Diskussion durch die Regierung auf Landesebene in Hinblick auf die Entwicklung geeigneter Richtlinien (parlamentarische Debatten etc.), und
 4. die Förderung von Forschung zum besseren Verständnis und Umgang mit dem Phänomen.

[...] Die Vorteile einer solchen Funktion leiten sich ab aus der besseren Konzeptualisierung von Trends, Anstrengungen und Strategien auf Staatsebene in Bezug auf den Menschenhandel, eingeschlossen wichtige Impulse für nationale Richtlinien und die nationale Gesetzgebung.

Ähnliche nicht-verbindliche Empfehlungen (sogenanntes „soft law“) zur Erhebung von Daten und zur Rolle der nationalen Berichterstattungsstelle wurden im Kontext der EU entwickelt. Am 4. Juni 2009 veröffentlichte der Europäische Rat bei der 2946. Tagung des Rates Justiz und Inneres ein Dokument mit Schlussfolgerungen zur Etablierung eines informellen EU-weiten Netzwerks nationaler Berichterstattungsstelle bzw. der vergleichbaren Mechanismen zum Menschenhandel:

- » 4. Basierend auf den existierenden EU-Instrumenten sollte das Netzwerk die vereinbarten Maßnahmen ergänzen, die von den existierenden EU-Strukturen durchgeführt werden. Insbesondere sollte sich das Netzwerk nicht in die Zusammenarbeit von Polizei und Justiz einmischen, etwa den Austausch von Untersuchungsergebnissen, inklusive personenbezogener Daten.

5. Jeder Mitgliedstaat ist auf Grundlage der Bedingungen auf Landesebene eingeladen, einen nationalen Berichtersteller oder gleichwertigen Mechanismus, dessen Aufgabe in der Sammlung von Informationen zu bzw. Beratung über den Menschenhandel besteht, zur Teilnahme an den Aktivitäten des Netzwerks zu bestimmen.

Am 19. Juni 2012 verabschiedete die EU-Kommission die „**Strategie der EU zur Beseitigung des Menschenhandels 2012–2016**“⁸². Die Strategie umfasst eine Reihe konkreter und praktischer Maßnahmen, die innerhalb von fünf Jahren umgesetzt werden sollen. Sie basiert auf fünf Schlüsselprioritäten:

- a. Erkennung, Schutz und Unterstützung der Betroffenen von Menschenhandel
- b. Verstärkung der Präventionsmaßnahmen gegen Menschenhandel
- c. Verstärkung der strafrechtlichen Verfolgung der Menschenhändler*innen
- d. Verbesserung der Koordination und Kooperation zwischen den maßgeblichen Akteuren sowie Kohärenz der Politiken
- e. Verbesserung der einschlägigen Kenntnisse und effiziente Reaktionen auf neu auftretende Probleme im Zusammenhang mit allen Formen des Menschenhandels

In Bezug auf die Instrumente zur Datenerhebung bezieht sich die EU-Strategie auf die rechtlich bindende EU-Richtlinie 2011/36/EU zur Verhütung und Bekämpfung des Menschenhandels und zum Schutz der von Menschenhandel Betroffenen. Alle Mitgliedstaaten sind zur Umsetzung der Richtlinie innerhalb eines klaren Zeitrahmens verpflichtet.

Die Eu schlägt verschiedene Vorgehensweisen vor, die im Folgenden dargestellt werden.

⁸² COM(2012) 286 final – Die Strategie der EU zur Beseitigung des Menschenhandels 2012–2016, 19. Juni 2012; http://ec.europa.eu/home-affairs/doc_centre/crime/docs/trafficking_in_human_beings_eradication-2012_2016_en.pdf .

Datenerhebungssysteme

Priorität E (Verbesserung der einschlägigen Kenntnisse und effiziente Reaktionen auf neu auftretende Probleme im Zusammenhang mit allen Formen des Menschenhandels) fordert als Maßnahme 1 die Entwicklung eines EU-weiten Datenerhebungssystems zur Sammlung verlässlicher und vergleichbarer Daten, damit Strategien zum Menschenhandel auf gesicherten Erkenntnissen und einem Verständnis der Ströme und Trends in EU-internen Menschenhandel aufbauen.⁸³ Der europäische Datenschutzbeauftragte (EDPS) hat die EU-Strategie überprüft und insbesondere folgende Punkte kommentiert:

- der Datenschutz als Vorbedingung für gegenseitiges Vertrauen zwischen den Betroffenen und den für Prävention, Schutz und Strafverfolgung zuständigen Behörden;
- der Datenschutz als Teil der Rechte von Betroffenen, insbesondere das Recht auf Information;
- der Datenschutz als Element eines EU-weiten Datenerhebungssystems;
- der Datenschutz als Strategie zur Unterstützung der Mitgliedstaaten beim Umgang mit Fragen bezüglich fundamentaler Rechte insbesondere in Verbindung mit Strategien zur Bekämpfung des Menschenhandels und damit in Zusammenhang stehender Aktivitäten.⁸⁴

Es ist eines der wenigen EU-Dokumente, das auf Datenschutzanliegen unter dem Aspekt von Empfehlungen zur Datenerhebung im Bereich der Menschenhandelsbekämpfung eingeht.

Der EDPS empfahl, dass die Strategie in der Umsetzungsphase stark von einer Ergänzung um eine Datenschutzperspektive und einer weiteren Klärung über die Art profitieren würde, wie der Datenschutz hier helfen könnte. Zudem betonte der EDPS, dass Informationen, die den Betroffenen von Menschenhandel zur Verfügung gestellt werden, nicht nur Informationen zum Recht auf den

83 Vgl. EU Strategie, S. 14.

84 Vgl. EDPS Kommentar unter: https://ec.europa.eu/anti-trafficking/sites/antitrafficking/files/edps_on_the_new_eu_anti-human_trafficking_strategy_1.pdf.

Schutz personenbezogener Daten, sondern auch über die Verfahren enthalten sollten, wie dieses Recht effektiv wahrgenommen werden kann⁸⁵.

Bestehende europäische und globale Instrumente zur Datenerhebung und Berichte

Während der letzten Jahre wurden auf der globalen und europäischen Ebene verschiedene Datenerhebungsverfahren entwickelt. Zwar zielen sie alle auf die quantitative Messung des Menschenhandels, unterscheiden sich aber sowohl in ihrer Methodik als auch in ihren Konzepten. Einige der globalen Datenerhebungsinstrumente erzeugen durch ihren direkten Einbezug in Aktivitäten zur Bekämpfung des Menschenhandels eigene Daten (beispielsweise die Datenerhebung durch die International Organization for Migration – IOM), andere bemühen sich um eine systematische Erfassung der bestehenden Daten, die ihnen von nationalen Berichterstattungsstelle und/oder einem ähnlichen Mechanismus zur Verfügung gestellt werden (das Außenministerium der Vereinigten Staaten, UNODC (United Nations Office on Drugs and Crime) und Eurostat (Statistische Amt der Europäischen Union). Ein weiterer Ansatz strebt danach, für Regierungen in einem nationalen Kontext ausgefeilte Richtlinien zur Datenerhebung auszuarbeiten (ICMPD – International Centre for Policy Development), und es bestehen Initiativen für methoden-basierte Schätzungen des globalen Ausmaßes von Menschenhandel und Zwangsarbeit (ILO). Diese Datensammlungsinstrumente können wie folgt chronologisch aufgelistet werden:

2001 begann das Außenministerium der USA allgemeine Daten zum Menschenhandel weltweit zu sammeln und die Wirkung von Strategien in den Bereichen Prävention, Schutz und Strafverfolgung zu evaluieren. Die Ergebnisse werden in dem globalen Bericht zum Menschenhandel TIP (Trafficking in Persons Report) veröffentlicht. Seit 2005 enthält der Bericht auch globale Zahlen zu identifizierten Betroffenen von Menschenhandel, Strafverfahren und Verurteilungen.

85 EDPS Kommentar, S. 5.

Das ICMPD entwickelte Datenerhebungsindikatoren zum Menschenhandel zur Umsetzung durch europäische Regierungen. Obwohl die Empfehlungen sich auf die nationale und die europäische Gesetzgebung zum Datenschutz beziehen, schlagen die ICMPD-Indikatoren dennoch die Erhebung personenbezogener Daten von Betroffenen von Menschenhandel vor.⁸⁶

Eine weitere führende internationale Organisation im Kampf gegen den Menschenhandel, die Internationale Organisation für Migration (IOM), führt eine globale Datenbank zum Menschenhandel:

- » Vor über einem Jahrzehnt hat IOM ein standardisiertes Instrument für die Verwaltung von Daten zum Menschenhandel aufgebaut und weiterentwickelt. Das sogenannte CTM (Counter-Trafficking Module) ist die weltweit größte Datenbank mit Primärdaten zu den Opfern des Menschenhandels.

CTM erleichtert alle Prozesse direkter Unterstützungsleistungen, Bewegungen und erneuter Integration der IOM durch ein zentral verwaltetes System, sowie durch die Aufzeichnung der Erfahrungen von Opfern des Menschenhandels. Im Gegenzug stärkt die Datenbank die Forschung und verbessert das Verständnis der Ursachen, Prozesse, Trends und Folgen des Menschenhandels. Sie dient als Wissensspeicher, aus dem sich Statistiken und detaillierte Berichte entwickeln lassen, und sie kann Informationen für die akademische Forschung sowie die Entwicklung von Programmen und Strategien zur Bekämpfung des Menschenhandels bereitstellen.

IOM stellt dabei sicher, dass Informationen, die den Persönlichkeitsbereich von Opfern des Menschenhandels verletzen oder deren Identität verraten könnte, in keinem Fall freigegeben werden. Zur Sicherstellung von Vertraulichkeit und der Sicherheit aller Daten bestehen strikte Kontrollen.⁸⁷

86 International Centre for Policy Development (Englisch); http://www.icmpd.org/fileadmin/ICMPD-Website/ICMPD_General/Publications/2009/DCIM-EU_Handbook.en.pdf.

87 Siehe englisches Zitat unter: <http://www.iom.int/cms/countertrafficking>.

2012 hat die Internationale Arbeitsorganisation (ILO) zum zweiten Mal eine Einschätzung der Anzahl der weltweit von Zwangsarbeit betroffenen Menschen veröffentlicht (die erste Schätzung fand 2005 statt). Die ILO schätzt, dass 2012 etwa 20,9 Millionen Menschen weltweit von Zwangsarbeit betroffen waren.⁸⁸ Allerdings basiert diese Schätzung nicht auf den Daten einer globalen Datenbank mit Primärdaten zu Menschen, die von der ILO als Zwangsarbeiter*innen identifiziert wurden, sondern beruht vielmehr auf einer Zusammenstellung von Informationen aus Sekundärquellen:

- » Die Methode basiert auf der globalen Sammlung ‚berichteter Fälle‘ von Zwangsarbeit in der Zeit zwischen 2002 und 2011. ‚Berichtete Fälle‘ bezieht sich auf spezifische Fälle von Zwangsarbeit, bei denen Ort und Zeit und die Anzahl der betroffenen Personen bekannt ist. Solche Fälle lassen sich in verschiedenen sekundären Quellen wie offiziellen Statistiken, Berichten von NGOs und Zeitungsartikeln finden.⁸⁹

2010 beauftragte die Generalversammlung der United Nations (UN) die UNODC mit der Erstellung eines globalen Berichts zu den Trends und Mustern des Menschenhandels.⁹⁰ 2012 veröffentlichte die UNODC einen solchen ersten globalen Bericht.⁹¹ Ähnlich wie die Strategie der EU zur Bekämpfung des Menschenhandels aus dem Jahr 2012 verzichtet auch

88 http://www.ilo.org/wcmsp5/groups/public/-ed_norm/-declaration/documents/publication/wcms_181953.pdf.

89 Siehe (Englisch): ILO 2012 Global Estimate of Forced Labour – Executive Summary, S. 5; http://www.ilo.org/wcmsp5/groups/public/-ed_norm/-declaration/documents/publication/wcms_181953.pdf.

90 Nach Paragraph 60 des Weltaktionsplans erhält die UNODC das Mandat und die Pflicht zur Sammlung relevanter Daten und Berichte zu den Mustern und den Strömen des Menschenhandels auf nationaler, regionaler und internationaler Ebene: „Den Generalsekretär zu ersuchen, mit Vorrang die Kapazität des Büros der Vereinten Nationen für Drogen- und Verbrechensbekämpfung dafür zu stärken, Informationen zu erheben und ab 2012 zweijährlich auf ausgewogene, zuverlässige und umfassende Weise und in enger Zusammenarbeit mit den Mitgliedstaaten über Muster und Ströme des Menschenhandels auf nationaler, regionaler und internationaler Ebene Bericht zu erstatten und aus verschiedenen Initiativen und Mechanismen abgeleitete bewährte Praktiken und Erkenntnisse auszutauschen“ (Resolution 64/293 der Generalversammlung, § 60). Siehe: www.unodc.org/unodc/en/human-trafficking-fund/hum.

91 Siehe: http://www.unodc.org/documents/data-and-analysis/glotip/Trafficking_in_Persons_2012_web.pdf.

der Bericht der UNODC auf die Nennung absoluter Zahlen für die weltweite Gesamtzahl von Betroffenen und Täter*innen und nennt stattdessen Prozentangaben. In Bezug auf die Methodologie nutzt der Bericht – genau wie der ILO-Bericht – sekundäre Quellen, darunter die Verbrechenstatistiken von Regierungen, die Jahresberichte von NROs usw.:

- » Der Großteil der für diesen Global Report on Trafficking in Persons gesammelten Daten stammt von den Institutionen einzelner Länder (88 Prozent der gesammelten Datenserien). Zu den weiteren Informationsquellen gehörten internationale Regierungsorganisationen (5 Prozent der Daten) und Nichtregierungsorganisationen (7 Prozent). Dabei basiert die Datenerhebung durch die UNODC auf drei verschiedenen Ansätzen. Erstens wurde ein knapper, eigens erstellter Fragebogen genutzt, der an Regierungen ausgegeben wurde. Zweitens wurden relevante Ergebnisse der regulären United Nations Survey of Crime Trends and Operations of Criminal Justice Systems zur Prüfung von Mitgliedstaaten durch offizielle Statistiken zu verschiedenen Formen von Kriminalität einbezogen. Drittens wurden schließlich im öffentlichen Raum verfügbare offizielle Informationen gesammelt (nationale Polizeiberichte, Berichte der Justizministerien, nationale Menschenhandelsberichte usw.).

Die Europäische Kommission hat in Zusammenarbeit mit Eurostat im Jahr 2013 erstmals statistische Daten zum Menschenhandel in den Mitgliedstaaten veröffentlicht. Hierbei werden die Fallzahlen in die Kategorien „identifizierte“ und „potentielle“ Betroffene von Menschenhandel unterteilt. Die fehlende Definition der beiden Kategorien stellt allerdings die Kohärenz der Statistiken in Frage. Für das Jahr 2010 ging der Bericht von insgesamt 9.582 identifizierten bzw. potentiell vom Menschenhandel Betroffenen in den EU-Mitgliedstaaten aus.⁹²

⁹² Siehe: http://ec.europa.eu/dgs/home-affairs/what-is-new/news/news/2013/docs/20130415_thb_stats_report_en.pdf, Seite 14.

Der Eurostat-Bericht beruht auch auf Sekundärdaten aus bereits bestehenden Statistiken der Mitgliedstaaten:

- » Im Einklang mit dem integrierten Ansatz zur Bekämpfung des Menschenhandels wurden Daten von verschiedenen zum Thema Menschenhandel tätigen Diensten und Organisationen in den teilnehmenden Ländern angefordert, wie Polizeistellen, Strafverfolgungsbehörden, Gerichten, Einwanderungsbehörden, Grenzschutz, Arbeitsaufsicht und Nicht-Regierungsorganisationen.

Die Fragebögen wurden im September 2011 von Eurostat an die nationalen Statistikinstitute der EU-Mitgliedstaaten, der EU-Beitrittskandidaten und der potenziellen Bewerberländer sowie an die EFTA/EEA-Länder (Europäische Freihandelsassoziation / Europäische Ökonomische Vereinigung) versandt. Sie enthielten geeignete Tabellen, eine Liste geläufiger Indikatoren, Definitionen und Leitlinien für die Erhebung statistischer Daten sowie die zu nutzenden Ländercodes und eine Vorlage zur Übersendung von Metadaten. Die von den beteiligten Ländern erhaltenen Daten wurden anschließend in Tabellen eingearbeitet und den Ländern im August 2012 zur Überprüfung geschickt. Im Dezember 2012 wurden die Tabellen von Eurostat fertiggestellt.⁹³

⁹³ Siehe: http://ec.europa.eu/dgs/home-affairs/what-is-new/news/news/2013/docs/20130415_thb_stats_report_en.pdf, Seite 21.

Weitere ausgewählte Datenbanken, Leitlinien und Werkzeuge der Datenerhebung:

- die globale Datenbank über Betroffene von Menschenhandel (Counter Trafficking Division, CTM) der IMO;
- Datenerhebung und Informationsmanagement (Data Collection and Information Management, DCIM) sowie die Leitlinien zur Datenerhebung des ICMPD;
- die Delphi-Befragung der ILO und der Europäischen Kommission;
- der UNODC - UN.GIFT Weltbericht zum Menschenhandel (beschreibt Muster und Ströme des Menschenhandels in 155 Ländern und Gebieten);
- die Entwicklung von Leitlinien zur Datenerhebung zum Menschenhandel, einschließlich vergleichbarer Indikatoren/ Variablen 2008 durch die IOM und das österreichische Innenministerium;
- the MONTRASEC demo (Universität Gent);
- das Europol-Informationssystem und die Europol-Arbeitsdatei zu Analysezwecken 'Phoenix' (AWF Phoenix 2007)



datACT-Empfehlungen

Kurz gesagt sind die Rechtsvorschriften zur Definition von Datenerhebungsinstrumenten wie Nationale Berichterstattungsstelle und/oder gleichwertigen Mechanismen (NREM) nach wie vor vage formuliert. Ebenso unklar ist die Einbindung von NROs bei Datenerhebungsverfahren. Die Bandbreite der existierenden Datenerhebungsmethoden behindert die Entwicklung klarer Handlungsleitlinien für Akteure. Hinsichtlich der Datenschutzbestimmungen zur Datenerhebung empfiehlt datACT die Einhaltung folgender Prinzipien:

- Die Berichterstattungsstelle sollte Datenschutzstandards garantieren und die Rechte der Datensubjekte schützen.
- Der Schutz der Privatsphäre der Betroffenen von Menschenhandel sollte im Mittelpunkt aller Datenschutzmaßnahmen stehen. Jegliche Datenerhebung muss auf Datenschutzmethoden wie dem „Privacy by Design“⁹⁴ und den „Privacy Impact Assessment“⁹⁵ basieren.
- Spezialisierte Fachberatungsstellen für Betroffene von Menschenhandel sollten nicht gezwungen werden, die Daten ihrer Klient*innen an staatlichen Instanzen oder Dritte weiterzugeben.
- Mandat und Zweck der Berichterstattungsstelle sollten auf klaren Kooperationsstandards zwischen den spezialisierten Fachberatungsstellen für Betroffene von Menschenhandel und den Berichterstattungsstellen basieren.
- Spezialisierte Fachberatungsstellen für Betroffene von Menschenhandel sollten als unabhängig Akteure agieren und dürfen von den ent-

94 Privacy by Design bedeutet, den Schutz der Privatsphäre von Anfang an zu berücksichtigen und direkt in die Gestaltungsvorgaben und den Aufbau neuer Verfahren und Prozesse zu integrieren.

95 Das Privacy Impact Assessment (PIA) ist eines von mehreren Instrumenten, das Organisationen dabei helfen soll zu gewährleisten, dass die während der Entwicklung eines Verfahrens oder Prozesses getroffenen Entscheidungen das Bedürfnis nach Schutz der Privatsphäre erfüllen, häufig anhand gezielter Fragestellungen zum Datenschutz.

sprechenden staatlichen und zwischenstaatlichen Instanzen nicht als Datenlieferant*innen missbraucht werden.

- Spezialisierte Fachberatungsstellen für Betroffene von Menschenhandel sollten von Datenschutzexpert*innen geschult werden, um ihre technische Ausstattung und Datenbanken zu kontrollieren und unautorisierten Zugang durch Dritte zu verhindern.
- Die Berichterstattungsstelle sollte unabhängig sein. Unabhängigkeit bedeutet hierbei nicht nur unabhängig von den gegenwärtigen staatlichen Verwaltungsinstanzen, sondern ebenfalls unabhängig von deren entsprechenden Mandaten und/oder Interessenskonflikten.
- Die Berichterstattungsstelle sollte regelmäßig von den nationalen Datenschutzbehörden und den nationalen Überwachungsgremien für Menschenrechte geprüft werden.
- Die Berichterstattungsstelle sollte keine operative Rolle im entsprechenden nationalen Weiterleitungsmechanismus (NRM) einnehmen.⁹⁶
- Die Datenerhebung durch die Berichterstattungsstelle sollte sich nicht nur auf den Menschenhandel allein beschränken, sondern auch die breiteren Rahmenbedingungen von Wirtschaftsordnung, Exklusion, Rassismus, Grenzkontrollen, Deregulierung der Arbeit etc. in Betracht ziehen.

96 „Ein nationales Leitsystem (National Referral Mechanism, NRM) ist ein Rahmen für die Zusammenarbeit, in dem staatliche Akteure ihren Verpflichtungen zum Schutz und zur Förderung der Menschenrechte der vom Menschenhandel Betroffenen in strategischer Zusammenarbeit mit der Zivilgesellschaft nachkommen. Grundlegende Ziele eines NRM sind die Gewährleistung der Menschenrechte der Betroffenen und die Schaffung effektiver Möglichkeiten, die Opfer an die entsprechenden Dienste weiterzuleiten. Zudem können NRMs dazu beitragen, die nationalen Strategien und Verfahren für ein breites Themenspektrum im Hinblick auf die Opfer zu verbessern, wie beispielsweise die Aufenthalts- und Rückführungsbestimmungen, die Opferentschädigung und den Zeugenschutz. NRMs können zur Einrichtung nationaler Aktionspläne führen und Maßstäbe setzen, um die Erreichung der Ziele zu überprüfen.“ (OSCE: National Referral Mechanisms – Joining efforts to protect the rights of trafficked persons, Warschau, 2004, Seite 15.)

5.2 Identifizierung der vom Menschenhandel betroffenen Personen und Zugang zu Unterstützungsstrukturen



Herausforderungen: Registrierung und Übermittlung der Daten von Betroffenen zwischen den Herkunfts- und Zielländern sowie unter den nationalen Behörden;

datACT-Empfehlungen:

- > Durchführung von Datenschutz-Folgenabschätzungen (Privacy-Impact-Assessments - PIA);
- > Bestimmung detaillierter Zielsetzungen und Zeitrahmen für die Erhebung von personenbezogenen Daten und weitestgehende Vermeidung unnötiger Übermittlungen personenbezogener Daten;
- > Beibehaltung und Befürwortung eines dezentralisierten und anonymen Zugangs zu Unterstützungsstrukturen für Betroffene von Menschenhandel.

Herausforderungen der Identifizierung

Potentiell vom Menschenhandel betroffene Personen werden von den Behörden aufgrund ihres irregulären Status, ihres möglichen Unwillen, das Verbrechen zur Anzeige zu bringen oder aufgrund der Einstellung der Ermittlungen, nicht immer als Opfer eines Verbrechens anerkannt. Dies hat ernsthafte Folgen für die potentiell Betroffenen, da ihnen die grundlegende Rechte auf Unterstützung und Schutz versagt bleiben, sie häufig verhaftet werden (infolge ihres irregulären Aufenthaltstitels) und/oder gegen sie aufgrund einer Straftat bzw. der Störung der öffentlichen Ordnung ermittelt wird, die sie im Zuge ihrer Tätigkeiten als von Menschenhandel Betroffene begangen haben.

Hinter der enormen Schere, die zwischen den offiziellen Fallzahlen zu Betroffenen des Menschenhandels und den Schätzungen internationaler Organisationen besteht, könnte die fehlende Anerkennung der Opfer als solche stehen, die wiederum Grundlage für die Nicht-Gewährung von Unterstützungsleistungen durch die Behörden ist. Als Ergebnis der Nicht-

Gewährung von Unterstützungsleistungen durch Behörden ist eine enorme Diskrepanz in den offiziellen Statistiken zu Menschenhandelsfällen und statistischen Schätzungen durch internationale Organisationen zu sehen.

Aus diesem Grund setzen internationale Akteure und Regierungen immer mehr auf politische Maßnahmen, die eine Identifizierung der Betroffenen durch Verwaltungsverfahren ermöglichen würden. Trotzdem ist im Palermo-Protokoll⁹⁷, das nur darauf verweist „die Durchführung von Maßnahmen [zu erwägen], welche die körperliche, seelische und soziale Gesundung der Opfer des Menschenhandels ermöglichen [...]“, kein Verfahren zur „Identifizierung der Opfer“ vorgesehen.⁹⁸ Das Palermo-Protokoll legt daher weder die Voraussetzungen fest, damit eine Person Unterstützung erhält, noch überträgt es den Behörden das Mandat zu entscheiden, ob eine potentiell vom Menschenhandel betroffene Person Zugang zu den Unterstützungsstrukturen erhält. Der Sprachgebrauch „Identifizierung der Opfer“ wurde auf UN-Ebene mit der Veröffentlichung des Dokuments „Empfohlene Grundsätze und Leitlinien zum Thema Menschenrechte und Menschenhandel“ (E/2002/68/Add) durch das Hochkommissariat für Menschenrechte gestärkt.⁹⁹ Hier wurde den Staaten die Entwicklung von Leitlinien empfohlen, „um die rasche und korrekte Identifizierung der Opfer von Menschenhandel zu ermöglichen“ (Leitlinie 2, Artikel 1).

Rund zehn Jahre nach dem Palermo-Protokoll legte die Annahme der EU-Richtlinie 2011/36/EU einige der Voraussetzungen für den Zugang zu Unterstützungsstrukturen der potentiell vom Menschenhandel Betroffenen fest.

- » Die Mitgliedstaaten treffen die erforderlichen Maßnahmen, um sicherzustellen, dass eine Person Unterstützung und Betreuung erhält, **sobald den zuständigen Behörden** berechtigte Gründe

97 Im Jahr 2000 wurde bei der UN-Kommission zur Verbrechensbekämpfung und Strafjustiz (Crime Commission) die Konvention zur Bekämpfung transnationaler Kriminalität und das sog. Palermo-Protokoll gezeichnet. In dieser bedeutenden Konvention wurde erstmals in einem völkerrechtlichen Vertrag eine detaillierte und international anerkannte Definition von Menschenhandel festgelegt: <http://www.unodc.org/unodc/treaties/CTOC/>.

98 Palermo-Protokoll Artikel 6 (3).

99 Dokument auf Englisch: <http://www.ohchr.org/Documents/Publications/Traffickingen.pdf>.

für die Annahme vorliegen, dass gegen diese Person eine der Straftaten gemäß Artikel 2 und 3 verübt worden sein könnte. (Artikel 11(2), eigene Hervorhebung)

Während die Opfer von anderen Gewaltverbrechen, einschließlich der Gewalt gegen Frauen, in der europäischen und internationalen Gesetzgebung nicht verpflichtend von den zuständigen Behörden als solche identifiziert werden müssen, um Zugang zu Strukturen für Unterstützung und Schutz zu erhalten, müssen die von Menschenhandel Betroffenen die zuständigen Stellen erst von ihrem Status als Opfer überzeugen, bevor sie auf angemessene Hilfe hoffen können.

Als Bedingung für den Zugang zu Unterstützungsstrukturen birgt die vorgeschaltete Identifizierung als Opfer Gefahren für das Recht auf Privatsphäre der potentiell von Menschenhandel Betroffenen. Da der Zugang zu Leistungen vornehmlich über die behördliche Verwaltungsebene läuft, haben die von Menschenhandel Betroffenen beispielsweise kaum Chancen auf eine anonyme Beratung. Somit gilt das Identifizierungsverfahren auch für Betroffene, die nicht mit den Strafverfolgungsbehörden zur Einleitung strafrechtlicher Ermittlungen zusammenarbeiten wollen. Wie an den folgenden zwei Beispielen in diesem Kapitel dargestellt, zielen die vorgeschlagenen Leitlinien zur Identifizierung vor allem auf die Erhebung personenbezogener und sensibler Daten des „zu identifizierenden“ potentiellen Opfers.

Obwohl die europäischen Länder über unterschiedliche verwaltungsrechtliche und gesetzliche Strukturen verfügen, um die von Menschenhandel Betroffenen zu identifizieren, bestehen doch zunehmend gemeinsame Anstrengungen, die Verfahren zur Identifizierung der Betroffenen auf überregionaler Ebene zu harmonisieren. Im Jahr 2013 regte die Europäische Kommission die Ausarbeitung des Referenzdokuments „Leitlinien zur Identifizierung der Opfer von Menschenhandel, insbesondere für Konsularstellen und Grenzkontrollen“ an.¹⁰⁰ Mit Bezug auf die EU-Strategie aus

¹⁰⁰ Siehe: http://ec.europa.eu/dgs/home-affairs/e-library/docs/thb-victims-identification/thb_identification_en.pdf.

dem Jahr 2012 unterstreicht die Kommission die Bedeutung einer „frühzeitigen Identifizierung“, indem sie eine Zusammenstellung von elf Projektzusammenfassungen zu Identifizierungsmethoden zur Verfügung stellt, die im Auftrag der Europäischen Kommission erstellt wurden.¹⁰¹ Ein wichtiger Teil der Identifizierungsleitlinien ist die Erhebung und Verarbeitung von Daten durch die zuständigen Behörden.¹⁰²

Die Leitlinien der Europäischen Kommission unterscheiden während des Identifizierungsverfahrens den Status des „potenziellen Opfers“ von dem des „identifizierten Opfers“. Diese Unterscheidung wird von EUROSTAT in der ersten EU-weiten Statistik zum Thema Menschenhandel von 2013 noch einmal bestätigt¹⁰³:

» Die Identifizierung der Opfer von Menschenhandel ist durch die nationalen Verfahren der Mitgliedstaaten bedingt:

Ein „identifiziertes Opfer“ ist eine Person, die formal von der zuständigen Behörde des Mitgliedstaates als Opfer von Menschenhandel identifiziert wurde.

Ein „mutmaßliches Opfer“ von Menschenhandel ist eine Person, auf welche die Kriterien der EU-Bestimmungen und internationalen Übereinkommen zutreffen, die jedoch noch nicht formal von den zuständigen Behörden (Polizei) als Opfer von Menschenhandel identifiziert wurde oder es ablehnt, formal oder legal als Opfer identifiziert zu werden.¹⁰⁴

In Zukunft zielen die Bemühungen der EU daher darauf ab, nicht nur jene Personen zu identifizieren, auf die der Indikator des „Opferprofils“ zutrifft, sondern auch jene Personen, die weder mit den Behörden zusammenarbeiten wollen noch ihrer Vermittlung in die Unterstützungsstrukturen zustimmen.

101 Siehe „Guidelines“, Seite 8–10.

102 Siehe „Guidelines“, Seite 6.

103 Hier muss angemerkt werden, dass die EU Kommission von ‚potential victims‘ spricht während Eurostat den Begriff ‚presumed victims‘ aufführt.

104 Siehe: http://ec.europa.eu/dgs/home-affairs/what-is-new/news/news/2013/docs/20130415_thb_stats_report_en.pdf, Seite 26.

Zusätzlich wurden mit dem Konzept der „länderübergreifenden Verweismechanismen“ (Transnational Referral Mechanisms, TRM), das vom Internationalen Zentrum für migrationspolitische Entwicklung (International Centre for Migration Policy Development, ICMPD)¹⁰⁵ erarbeitet wurde, grenzüberschreitende Verfahren zur Identifizierung von Opfern eingeführt. Unlängst fand der Begriff auch Eingang in die Strategie der EU:

Transnational Referral Mechanisms (Länderübergreifende Verweismechanismen)

Priorität A (Erkennung, Schutz und Unterstützung der Opfer des Menschenhandels) diktiert in seiner Maßnahme 1 die Einrichtung nationaler und länderübergreifender Verweismechanismen. Die länderübergreifenden Mechanismen sollten bis 2015 ein Verfahren beschreiben, die zur besseren Erkennung, Verweisung und Unterstützung von Opfern führen und die entsprechenden Behörden sowie die Zivilgesellschaft mit einbeziehen.¹⁰⁶

Die Identifizierungsprozesse basieren auf intensiven Dokumentations- und Registrierungsverfahren der potentiell vom Menschenhandel betroffenen Personen. Zudem empfiehlt der länderübergreifende Verweismechanismus, eine „formale Identifizierung“ der Betroffenen durch die zuständigen Behörden vorzunehmen. Nach diesem Konzept ist eine „formale Identifizierung“ durch die Behörden weder an strafrechtliche Ermittlungen noch an die Bereitschaft des Opfers zur Zusammenarbeit mit den Strafverfolgungsbehörden geknüpft. Der Abschluss der „formalen Identifizierung“ würde den Opfern Zugang zu weiteren Diensten, einschließlich Unterstützung, Schutz und sozialer Inklusion ermöglichen.¹⁰⁷ Das ICMPD beschreibt sechs Maßnahmen des Identifizierungsprozesses:

105 Siehe: http://www.icmpd.org/fileadmin/ICMPD-Website/ICMPD-Website_2011/Capacity_building/THB/Publications/TRM_EU_guidelines.pdf .

106 Strategie der EU zur Beseitigung des Menschenhandels 2012–2016, COM(2012) 286 final, Seite 6, siehe unter: http://ec.europa.eu/home-affairs/doc_centre/crime/docs/trafficking_in_human_beings_eradication-2012_2016_en.pdf .

107 Siehe „ICMPD Guidelines for TRM“, Seite 56; <http://www.icmpd.org/Trafficking-in-Human-Beings.2443.0.html> .

- „erste Prüfung und Verweisung;
- Zugang zu Grundversorgung und Informationen;
- frühe Risikoabschätzung;
- Sprachmittlung und kulturelle Mediation;
- Phase der Erholung und Reflexion;
- Identifizierung“.¹⁰⁸

Für den Datenschutz ist das Konzept des länderübergreifenden Verweismechanismus im Umgang mit den Daten der vom Menschenhandel Betroffenen eine große Herausforderung. In den frühen Kriterien zur Risikobewertung empfiehlt das Konzept nicht nur die Erhebung von personenbezogenen Daten, sondern auch Daten zum Gesundheitszustand der Betroffenen.¹⁰⁹

Aus diesem Grund hat der Europäische Datenschutzbeauftragte (EDSB) angeregt, Informationen darüber, wie das Recht auf Schutz der personenbezogenen Daten konkret genutzt werden kann, sowie die Arbeit der nationalen Datenschutzbehörden in die nationalen und länderübergreifenden Verweismechanismen aufzunehmen.¹¹⁰



datACT Empfehlungen:

Im Allgemeinen gilt: Wird eine Datenerhebung zur Voraussetzung für den Zugang zu Unterstützungsstrukturen, sollten die Maßnahmen zur Bekämpfung von Menschenhandel den Zweck derselben klar bestimmen. Dem Zweck sollten legitime Interessen zu Grunde liegen. Die Verarbeitung personenbezogener Daten ist von der freien Zustimmung nach erfolgter Aufklärung des „Datensubjekts“ – sprich der vom Menschenhandel betroffenen Person – abhängig.

¹⁰⁸ Siehe „ICMPD Guidelines for TRM“, Seite 34.

¹⁰⁹ Siehe „ICMPD Guidelines for TRM“, Seite 43.

¹¹⁰ Anmerkungen des EDSB zur Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen – „Die Strategie der EU zur Beseitigung des Menschhandels 2012–2016“, S. 4; https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Comments/2012/12-07-10_Human_Trafficking_DE.pdf.

Die bestehenden Spannungen zwischen den Rechten der betroffenen Person und den Pflichten der für die Verarbeitung der Daten verantwortlichen Person lässt sich wie folgt darstellen:



Empfohlene Grundsätze der Datenerhebung für (nicht-staatliche) Fachberatungsstelle bei der Erstberatung:

- > Die Erhebung von personenbezogenen Daten der von Menschenhandel Betroffenen muss auf ein absolutes Mindestmaß beschränkt werden. Der Zweck der Datenerhebung sollte reflektiert und in Einklang mit den bestehenden europäischen und deutschen Datenschutzbestimmungen erfolgen.
- > Personenbezogene Daten, die mit einem bestimmten Zweck erhoben wurden, sollten weder zu anderen Zwecken gespeichert, noch mit Außenstehenden oder Dritten geteilt werden.
- > In Zusammenarbeit mit den Mitarbeiter*innen von spezialisierten Fachberatungsstellen für Betroffene von Menschenhandel sollten Indikatoren entwickelt werden, die den Zugang der potentiell von Menschenhandel Betroffenen zu den Fachberatungsstellen regeln.
- > Diese Indikatoren sollten individuelle Entscheidungen durch die Berater*innen über die Aufnahme mutmaßlicher Opfer in die Unterstützungsstrukturen weder aufheben noch ersetzen. Die Indikatoren sollten die tägliche Beratungsarbeit erleichtern.

- Potentiell von Menschenhandel betroffenen Personen soll ein niedrigschwelliger Zugang zu anonymer Beratung ermöglicht werden. Vereinfachte Zugangsmöglichkeiten sind für die Herstellung eines Erstkontakts für potentiell betroffene Personen von höchster Bedeutung, um sie über mögliche weitere Schritte zu informieren.
- Europaweit sollte eine mindestens dreimonatige Bedenkfrist für Betroffene von Menschenhandel eingeführt werden, um potentiell Betroffenen das Handeln und Entscheiden im eigenen Interesse zu ermöglichen. Diese Zeitspanne sollte als Bedenk- und Stabilisierungsfrist verstanden werden, die unabhängig von der Kooperationsbereitschaft der Betroffenen im Strafverfahren garantiert werden muss.

Empfohlene Grundsätze für Rückkehr in Herkunftsländer/soziale Wiedereingliederung:

- Jede grenzüberschreitende Weitergabe personenbezogener Daten der von Menschenhandel betroffenen Personen sollte vermieden werden.
- Es muss von allen Beteiligten sichergestellt werden, dass die Identität der Betroffenen von Menschenhandel nach ihrer Rückkehr und den Wiedereingliederungsmaßnahmen nicht zurückverfolgt werden kann.

5.3 Datenschutz und spezialisierte Fachberatungsstellen für Betroffene von Menschenhandel



Herausforderungen: Internationale EDV-gestützte Falldokumentation und Verwaltungssysteme könnten unsicher sein; nicht-staatliche Fachberatungsstellen könnten sich gezwungen sehen, Strafverfolgungsinstanzen Informationen zu übermitteln; die Rechte der Opfer als Datensubjekte könnten nicht integraler Bestandteil des Beratungsprozesses sein.

datACT Empfehlungen :

- > Einführung sicherer Soft- und Hardware in nicht-staatlichen Fachberatungsstellen, im Anschluss an eine Datenschutz-Folgeabschätzung (PIA);
- > Eintreten für einen strengeren Schutz der Schweigepflicht und des Aussageverweigerungsrechts vor Gericht;
- > Einführung von Beratungsmodulen zum Recht auf Privatsphäre

Wie in den vorausgehenden Kapiteln schon angesprochen, können nicht-staatliche Fachberatungsstellen für Betroffene von Menschenhandel gezwungen sein, Informationen über Hilfesuchende – einschließlich personenbezogener Daten – an Behörden oder andere Akteure weiterzugeben. Selbst wenn die von Menschenhandel betroffene Person nicht mit den Strafverfolgungsbehörden zusammenarbeitet, kann es während des Beratungsprozesses aus folgenden Gründen zum Datenaustausch mit Behörden und weiteren Dritten kommen:

- Erteilung einer Bedenkfrist und Aufenthaltsgenehmigung;
- Beantragung von Sozialleistungen;
- Verpflichtungen gegenüber Geldgeber*innen, einschließlich Jahresberichten und Statistiken;
- Zusammenarbeit mit Nationalen Berichterstattungsstellen und/oder gleichwertigen Mechanismen;
- Vorbereitung der Rückkehr ins oder von Maßnahmen zur sozialen Inklusion im Herkunftsland;
- Andere Bemühungen.

Internationale, regionale und nationale Richtlinien- und Rechtsdokumente enthalten nur vage Angaben über die Art der Zusammenarbeit der Zivilgesellschaft mit den Behörden und der Rolle, die sie bei der Erhebung von Daten und dem Datenschutz spielt. Aus diesem Grund bedürfen die Leitlinien für nicht-staatliche Verarbeiter*innen von personenbezogenen Daten von vom Menschenhandel Betroffener künftig weiterer Ausarbeitung. Dasselbe gilt für die Rolle von NROs im Rahmen der nationalen und internationalen Datenerhebungsverfahren, wie die der Nationalen Berichterstattungsstellen und/oder gleichwertigen Mechanismen. Die EU-Richtlinie 2011 empfiehlt die Zusammenarbeit von Zivilgesellschaft und Nationalen Berichterstattungsstellen, versäumt es jedoch, die Rolle und das Mandat der NROs in diesem Zusammenhang zu definieren. Das folgende Beispiel eines Privacy Impact Assessment (PIA) könnte das Feld aufzeigen, anhand dessen sich die Rolle und die Pflichten von nicht-staatlichen Dienstleister*innen in Hinblick auf die Datenschutzbestimmungen eindeutiger definieren lassen.

Artikel 6: Grundsätze in Bezug auf die Qualität der Daten¹¹¹

1. Die Mitgliedstaaten sehen vor, dass personenbezogene Daten:
 - a) nach Treu und Glauben und auf rechtmäßige Weise verarbeitet werden;



Fragen für eine PIA für Fachberatungsstellen zum Thema Menschenhandel:¹¹²

- Existiert innerhalb des Beratungsangebots der Beratungsstelle die Möglichkeit zu einer anonymen Erstberatung?
- Wurden Richtlinien zur Datenverarbeitung innerhalb der Beratungsstelle diskutiert und festgelegt?
- Wie werden die Klient*innen (Betroffene von Menschenhandel) über die Nutzung ihrer personenbezogenen Daten informiert?

¹¹¹ Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, Amtsblatt Nr. L 281 vom 23/11/1995 S. 0031 – 0050.

¹¹² Die Fragen wurden leicht abgewandelt dem Praxishandbuch des ICO entnommen: Information Commissioner's Office: Conducting privacy impact assessments, code of practice. Februar 2014, Seite 39.

- Sollte dem Aspekt der Privatsphäre innerhalb der Beratung ein höherer Stellenwert eingeräumt werden?
 - Wurden Bedingungen für die Verarbeitung personenbezogener Daten der Klient*innen (Betroffenen von Menschenhandel) festgelegt?
 - Werden innerhalb des Verarbeitungsprozesses personenbezogene Daten durch Akronyme oder IdentifizierungsCodes verschlüsselt?
 - Wie findet innerhalb der Beratungsstelle der interne Austausch zwischen Mitarbeiter*innen statt?
-

b) für festgelegte, eindeutige und rechtmäßige Zwecke erhoben und nicht in einer mit diesen Zweckbestimmungen nicht zu vereinbarenden Weise weiterverarbeitet werden. Die Weiterverarbeitung von Daten zu historischen, statistischen oder wissenschaftlichen Zwecken ist im Allgemeinen nicht als unvereinbar mit den Zwecken der vorausgegangenen Datenerhebung anzusehen, sofern die Mitgliedstaaten geeignete Garantien vorsehen;



Fragen für eine PIA für Fachberatungsstellen zum Thema Menschenhandel¹¹³:

- Wurden innerhalb der Beratungsstelle Grund und Zweck der Datensammlung bestimmt?
 - Wurden im Verlauf der letzten Jahre neue Zwecke und ein erhöhter Bedarf an personenbezogenen Daten von Klient*innen identifiziert?
-

c) den Zwecken entsprechen, für die sie erhoben und/oder weiterverarbeitet werden, dafür erheblich sind und nicht darüber hinausgehen;



Fragen für eine PIA für Fachberatungsstellen zum Thema Menschenhandel:¹¹⁴

- Werden über den benötigten Zweck hinaus Daten von Klient*innen erhoben und verarbeitet?
-

113 Ebd.

114 Ebd.

- d) sachlich richtig und, wenn nötig, auf den neuesten Stand gebracht sind; es sind alle angemessenen Maßnahmen zu treffen, damit im Hinblick auf die Zwecke, für die sie erhoben oder weiterverarbeitet werden, nicht zutreffende oder unvollständige Daten gelöscht oder berichtigt werden;



Fragen für eine PIA für Fachberatungsstellen zum Thema Menschenhandel:¹¹⁵

- Wie wird sichergestellt, dass Daten korrigiert oder gelöscht werden können?

- e) nicht länger, als es für die Realisierung der Zwecke, für die sie erhoben oder weiterverarbeitet werden, erforderlich ist, in einer Form aufbewahrt werden, die die Identifizierung der betroffenen Personen ermöglicht. Die Mitgliedstaaten sehen geeignete Garantien für personenbezogene Daten vor, die über die vorgenannte Dauer hinaus für historische, statistische oder wissenschaftliche Zwecke aufbewahrt werden.



Fragen für eine PIA für Fachberatungsstellen zum Thema Menschenhandel:¹¹⁶

- In welcher Form werden personenbezogene Daten von Klient*innen in der Beratungsstelle gespeichert und aufbewahrt?
- Wie lange werden personenbezogene Daten von Klient*innen innerhalb der Beratungsstelle gespeichert?
- Erlaubt die verwendete Software das Löschen der Informationen gemäß dem jeweils vorgesehenen Aufbewahrungszeitraum?

-
2. Der für die Verarbeitung Verantwortliche hat für die Einhaltung des Absatzes 1 zu sorgen.

115 Ebd.

116 Ebd.

Artikel 7: Grundsätze in Bezug auf die Zulässigkeit der Verarbeitung von Daten

Die Mitgliedstaaten sehen vor, dass die Verarbeitung personenbezogener Daten lediglich erfolgen darf, wenn eine der folgenden Voraussetzungen erfüllt ist:

- a) Die betroffene Person hat ohne jeden Zweifel ihre Einwilligung gegeben;
- b) die Verarbeitung ist für die Erfüllung eines Vertrags erforderlich, dessen Vertragspartei die betroffene Person ist, oder für die Durchführung vorvertraglicher Maßnahmen, die auf Antrag der betroffenen Person erfolgen;
- c) die Verarbeitung ist für die Erfüllung einer rechtlichen Verpflichtung erforderlich, der der für die Verarbeitung Verantwortliche unterliegt;
- d) die Verarbeitung ist erforderlich für die Wahrung lebenswichtiger Interessen der betroffenen Person;
- e) die Verarbeitung ist erforderlich für die Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt und dem für die Verarbeitung Verantwortlichen oder dem Dritten, dem die Daten übermittelt werden, übertragen wurde;
- f) die Verarbeitung ist erforderlich zur Verwirklichung des berechtigten Interesses, das von dem für die Verarbeitung Verantwortlichen oder von dem bzw. den Dritten wahrgenommen wird, denen die Daten übermittelt werden, sofern nicht das Interesse oder die Grundrechte und Grundfreiheiten der betroffenen Person, die gemäß Artikel 1 Absatz 1 geschützt sind, überwiegen.



Fragen für eine PIA für Fachberatungsstellen zum Thema Menschenhandel:¹¹⁷

- Werden im Verlauf der Beratung Einverständniserklärungen der Klient*innen zur Verarbeitung ihrer Daten eingeholt?
- Werden Klient*innen in der fortlaufenden Beratung über den Gebrauch und die Speicherung ihrer Daten informiert?
- Was wird im Falle von zurückgehaltenen oder widersprochenen Einwilligungserklärungen unternommen?

¹¹⁷ Ebd.

- Welche Daten müssen aufgrund der Kooperation mit Behörden/Institutionen gesammelt werden (Bsp.: Anträge auf Leistungsbezug)?
- Existieren Kooperationsvereinbarungen mit Behörden/Institutionen, die den Umfang und die Form der zu übermittelnden Daten festlegen?
- Werden Ihre Maßnahmen im Widerspruch zum Recht auf Datenschutz stehen?
- Wurden die gesellschaftliche Notwendigkeit und die Ziele des Projekts bestimmt?
- Ist das Vorgehen eine angemessene Antwort auf die gesellschaftliche Notwendigkeit?

Artikel 1 (1) der Datenschutzrichtlinie erläutert den Gegenstand der Richtlinie:

- » Die Mitgliedstaaten gewährleisten nach den Bestimmungen dieser Richtlinie den Schutz der Grundrechte und Grundfreiheiten und insbesondere den Schutz der Privatsphäre natürlicher Personen bei der Verarbeitung personenbezogener Daten.



Fragen für eine PIA für Fachberatungsstellen zum Thema Menschenhandel:¹¹⁸

- Besitzt der/die IT-Dienstleister* in oder technische Leitung der Datenbank Zugang zu personenbezogenen Daten?
 - Wird die Beratungsstelle im Rahmen von Rückkehrprogrammen und internationaler Zusammenarbeit zur Weitergabe von Daten ins (europäische) Ausland angefragt?
 - Findet in Fällen der Zusammenarbeit mit Rückkehrprogrammen eine Weitergabe personenbezogener Daten statt?
 - Wie wird im Falle einer Datenweitergabe der adäquate Schutz der Daten sichergestellt?
 - Werden Klient*innen (Betroffenen von Menschenhandel) über die Ansprechpartner*innen im Falle eines gewünschten Zugangs zu ihren personenbezogenen Daten informiert?
 - Existiert eine Zusammenarbeit mit der zuständigen Datenschutzbehörde?
 - Wurde bereits geprüft, ob eine/ein Datenschutzbeauftragte/r zu bestellen ist?
-



datACT-Empfehlungen:

Datenschutz und Datensammlung in der weiterführenden Beratung

- Spezialisierte Fachberatungsstellen für Betroffene von Menschenhandel sollten sich dafür einsetzen und zugleich überwachen, dass die Sammlung personenbezogener Daten durch staatliche Behörden und zwischenstaatliche Organisationen auf ein absolutes Minimum reduziert wird.
- Personenbezogene Daten sollten nach Möglichkeit mit Hilfe von Akronymen oder Identifizierungs-codes durch die Beratungsstelle verschlüsselt werden, sofern die personellen und finanziellen Ressourcen innerhalb der spezialisierten Fachberatungsstelle für Betroffene von Menschenhandel gegeben sind.
- Spezialisierte Fachberatungsstellen sollten in Kooperation mit IT-Datenschutzexpert*innen sichere Computersoftware und Hardware für ihr Falldokumentationssystem entwickeln und installieren. Cloud computing services und ein Online-Zugang zu den Fallakten sollte vermieden werden.
- Jedweder Kooperation mit Behörden oder Dritten sollte nach Möglichkeit ein Austausch mit der/dem zuständigen Datenschutzbeauftragten vorausgehen und auf einer Vereinbarung zum strikten Gebrauch vollständig anonymisierter Daten beruhen.
- Das Zeugnisverweigerungsrecht für Mitarbeiter*innen von spezialisierten Fachberatungsstellen für Betroffene von Menschenhandel gegenüber Behörden und Gerichten sollte europaweit eingeführt und jeder Mitarbeiter*in zugesprochen werden.¹¹⁹
- Interne Beratung und der Austausch zu den jeweiligen Fällen sollten nach Möglichkeit nicht schriftlich festgehalten werden, sondern auf verbaler Kommunikation beruhen.

¹¹⁹ Vorschlag des KOK e.V. über die strafprozessuale Einführung eines Zeugnisverweigerungsrechtes für Mitarbeitende von spezialisierten Fachberatungsstellen für Betroffene von Menschenhandel gemäß § 53 StPO.

- Der Zweck der Sammlung und Speicherung von Daten sollte klar definiert und der Zeitraum der Speicherung und der Zeitpunkt der Löschung der Daten benannt werden.
- Nur befugte Mitarbeiter*innen von spezialisierten Beratungsstellen sollten Zugang zu Fallakten mit personenbezogenen Daten potentiell Betroffener erhalten.
- Alle Aktivitäten zur Datensammlung sollten auf Methoden des Datenschutzes beruhen, so wie „Privacy by Design“¹²⁰ und „Privacy Impact Assessment“¹²¹.

Beratung zum Datenschutz

- Die Rechtsansprüche auf Schutz der persönlichen Daten von potentiell Betroffenen von Menschenhandel sollten integraler Bestandteil der Beratungsarbeit sein.
- Potentiell Betroffene von Menschenhandel sollten in jedem Schritt über den Gebrauch und die Speicherung der ihren Fall betreffenden Daten informiert werden.
- Potentiell Betroffene von Menschenhandel sollten schriftlich ihr Einverständnis zu Sammlung und Verarbeitung ihrer Daten erklären.
- Spezialisierte Fachberatungsstellen sollten potentiell Betroffene von Menschenhandel über ihre Ansprechpartner*innen im Falle eines gewünschten Zugangs personenbezogener Daten informieren.

120 „Privacy by Design“ beinhaltet die Annahme, dass die Privatsphäre in Zukunft nicht allein durch rechtliche und regulierende Rahmenkonzepte gesichert werden kann. Der Schutz der Privatsphäre muss die Grundlage jedes organisatorischen oder institutionellen Handelns sein.

121 2009 erstellte die Europäische Kommission die Empfehlung „Commission Recommendation on the implementation of privacy and data protection principles in applications supported by radio-frequency identification“ zur Durchführung von Beurteilungen der Auswirkungen auf und Risiken für die Privatsphäre.

ANHANG I

RECHTEKATALOG DER DATENSUBJEKTE ZUR AUFNAHME IN DIE NRO-BERATUNGSARBEIT

WELCHE RECHTE HABEN SIE?

Allgemeines Recht

Einzelpersonen sind durch ein allgemeines Recht geschützt, demzufolge personenbezogene Daten fair und rechtmäßig und nur zu legitimen Zwecken verarbeitet werden dürfen.

Spezifische Rechte

Dieses allgemeine Recht wird durch eine Reihe spezifischer Individualrechte ergänzt:

- das Recht, zu erfahren, ob ein staatliches Organ oder eine Einrichtung Sie betreffende Daten verarbeitet;
- das Recht auf Informationen über die spezifische Verarbeitung (welche Informationen verarbeitet werden);
- das Recht, aus zwingenden und legitimen Gründen gegen die Verarbeitung Widerspruch einzulegen;
- das Recht auf Auskunft (z. B. über die Identität der für die Verarbeitung verantwortlichen Person, den Zweck der Verarbeitung, die Empfänger*innen der Daten);
- Recht auf Einsicht der eigenen personenbezogenen Daten;
- Berichtigung unrichtiger, nicht aktueller oder unvollständiger Daten;
- Sperrung von Daten, deren Richtigkeit bestritten wird;
- Löschung von Daten, wenn ihre Verarbeitung rechtswidrig ist;
- Mitteilung jeder Löschung, Berichtigung oder Sperrung der eigenen Daten gegenüber Dritten, denen die Daten übermittelt wurden;
- das Recht, einer solchen Übermittlung zu widersprechen;
- das Recht auf Schadensersatz.

Welche Verantwortung tragen Sie für den Schutz Ihrer personenbezogenen Daten?

- Überlegen Sie gut, ob sie Ihre Daten offenlegen;
- Machen Sie ausschließlich Angaben, die von der beteiligten Organisation benötigt werden;
- Hinterfragen Sie, warum Sie um eine spezifische persönliche Information gebeten werden.

ANHANG II

DATENSCHUTZSTANDARDS FÜR SPEZIALISIERTE NRO- FACHBERATUNGSSTELLEN FÜR BETROFFENE VON MENSCHENHANDEL

Die datACT-Standards entstanden in enger Kooperation mit den 37 Mitgliedsorganisationen des KOK e.V. und den acht europäischen Partnerorganisationen von La Strada International während der regelmäßig stattfindenden Mitgliederversammlungen und Netzwerktreffen sowie auf der Mitgliederversammlung der Global Alliance against Trafficking in Women (GAATW) in Bangkok, Thailand.

Auf Grundlage europäischen Datenschutzrechts und der Rückmeldungen aus der Praxis wurden Datenschutzstandards für spezialisierte Fachberatungsstellen entwickelt, die in der alltäglichen Beratungsarbeit als Richtlinien zum Schutz der Daten von Betroffenen des Menschenhandels und zur Verbesserung bestehender Datenschutzverfahren dienen sollen. Sie sind nicht als festes Regelwerk zu verstehen, sondern als Empfehlungen für den Umgang mit personenbezogenen Daten und sollen zum Thema Datenschutz in der Politik zur Bekämpfung des Menschenhandels sensibilisieren.

Die Datenschutzstandards sind kein starres und endgültiges Dokument, sondern entwickeln sich durch die Erfahrungen und Einschätzungen erfahrener Berater*innen stetig weiter.

1. Grundlegende Prinzipien des Datenschutzes bei der Erstberatung

- Die Erhebung von personenbezogenen Daten der von Menschenhandel Betroffenen muss auf ein absolutes Mindestmaß beschränkt werden. Der Zweck der Datenerhebung sollte reflektiert und in Einklang mit den bestehenden europäischen und deutschen Datenschutzbestimmungen erfolgen.
- Personenbezogene Daten, die zu einem bestimmten Zweck erhoben wurden, sollten weder zu anderen Zwecken gespeichert noch mit Außenstehenden oder Dritten geteilt werden.
- In Zusammenarbeit mit den Mitarbeiter*innen von spezialisierten Fachberatungsstellen für Betroffene von Menschenhandel sollten Indikatoren entwickelt werden, die den Zugang der potentiell von Menschenhandel Betroffenen zu den Fachberatungsstellen regeln.
- Diese Indikatoren sollten die individuelle Entscheidung durch die Berater*innen über die Aufnahme potentiell Betroffener von Menschenhandel in die Unterstützungsstrukturen weder aufheben noch ersetzen. Die Indikatoren sollen die tägliche Beratungsarbeit erleichtern.

- Potentiell von Menschenhandel betroffenen Personen sollte ein niedrighschwelliger Zugang zu anonymer Erstberatung ermöglicht werden. Vereinfachte Zugangsmöglichkeiten sind für die Herstellung eines Erstkontakts für potentiell betroffene Personen von höchster Bedeutung, um sie über mögliche weitere Schritte zu informieren.
- Europaweit sollte eine mindestens dreimonatige Bedenkfrist für Betroffenen von Menschenhandel eingeführt werden, um potentiell Betroffenen das Handeln und Entscheiden im eigenen Interesse zu ermöglichen. Diese Zeitspanne sollte als Bedenk- und Stabilisierungsfrist verstanden werden, die unabhängig von der Kooperationsbereitschaft der Betroffenen im Strafverfahren garantiert werden muss.

2. Datenschutz und Datensammlung in der weiterführenden Beratung

- Spezialisierte Fachberatungsstellen für Betroffene von Menschenhandel sollten sich dafür einsetzen und zugleich überwachen, dass die Sammlung personenbezogener Daten durch staatliche Behörden und zwischenstaatliche Organisationen auf ein absolutes Minimum reduziert wird.
- Personenbezogene Daten sollten nach Möglichkeit mit Hilfe von Akronymen oder Identifizierungs-codes durch die Beratungsstelle verschlüsselt werden, sofern die personellen und finanziellen Ressourcen innerhalb der spezialisierten Fachberatungsstelle für Betroffene von Menschenhandel gegeben sind.
- Spezialisierte Fachberatungsstellen sollten in Kooperation mit IT-Datenschutzexpert*innen sichere Computersoftware und Hardware für ihr Falldokumentationssystem entwickeln und installieren. Cloud computing services und ein Online-Zugang zu den Fallakten sollte vermieden werden.
- Jedweder Kooperation mit Behörden oder Dritten sollte nach Möglichkeit ein Austausch mit der/dem zuständigen Datenschutzbeauftragten vorausgehen und auf einer Vereinbarung zum strikten Gebrauch vollständig anonymisierter Daten beruhen.

- Das Zeugnisverweigerungsrecht für Mitarbeiter*innen von spezialisierten Fachberatungsstellen für Betroffene von Menschenhandel gegenüber Behörden und Gerichten sollte europaweit eingeführt und jeder* jedem Mitarbeiter* in zugesprochen werden¹.
- Interne Beratung und der Austausch zu den jeweiligen Fällen sollten nach Möglichkeit nicht schriftlich festgehalten werden, sondern auf verbaler Kommunikation beruhen.
- Der Zweck der Sammlung und Speicherung von Daten sollte klar definiert und der Zeitraum der Speicherung und der Zeitpunkt der Löschung der Daten benannt werden.
- Nur befugte Mitarbeiter*innen von spezialisierten Beratungsstellen sollten Zugang zu Fallakten mit personenbezogenen Daten potentiell Betroffener erhalten.
- Alle Aktivitäten zur Datensammlung sollten auf Methoden des Datenschutzes beruhen, so wie „Privacy by Design“² und „Privacy Impact Assessment“³.

1 Vorschlag des KOK e.V. über die strafprozessuale Einführung eines Zeugnisverweigerungsrechtes für Mitarbeitende von spezialisierten Fachberatungsstellen für Betroffene von Menschenhandel gemäß § 53 StPO.

2 „Privacy by Design“ beinhaltet die Annahme, dass die Privatsphäre in Zukunft nicht allein durch rechtliche und regulierende Rahmenkonzepte gesichert werden kann. Der Schutz der Privatsphäre muss die Grundlage jedes organisatorischen oder institutionellen Handelns sein.

3 2009 erstellte die Europäische Kommission die Empfehlung „Commission Recommendation on the implementation of privacy and data protection principles in applications supported by radio-frequency identification“ zur Durchführung von Beurteilungen der Auswirkungen auf und Risiken für die Privatsphäre.

3. Beratung zum Datenschutz

- Die Rechtsansprüche auf Schutz der persönlichen Daten von potentiell Betroffenen von Menschenhandel sollten integraler Bestandteil der Beratungsarbeit sein.
- Potentiell Betroffene von Menschenhandel sollten in jedem Schritt über den Gebrauch und die Speicherung der ihren Fall betreffenden Daten informiert werden.
- Potentiell Betroffene von Menschenhandel sollten schriftlich ihr Einverständnis zu Sammlung und Verarbeitung ihrer Daten erklären.
- Spezialisierte Fachberatungsstellen sollten potentiell Betroffene von Menschenhandel über ihre Ansprechpartner*innen im Falle eines gewünschten Zugangs personenbezogenen Daten informieren.

4. Datenschutz und die Rückkehr in Herkunftsländer/ soziale Wiedereingliederung

- Jede grenzüberschreitende Weitergabe personenbezogener Daten der von Menschenhandel betroffenen Personen sollte vermieden werden.
- Es muss von allen Beteiligten sichergestellt werden, dass die Identität der Betroffenen von Menschenhandel nach ihrer Rückkehr und den Wiedereingliederungsmaßnahmen nicht zurückverfolgt werden kann.

5. Standards für die Einrichtung einer nationalen Berichterstattung oder gleichwertiger Mechanismen

- Die Berichterstattungsstelle sollte Datenschutzstandards garantieren und die Rechte der Datensubjekte schützen.
- Der Schutz der Privatsphäre von Betroffenen von Menschenhandel sollte im Mittelpunkt aller Datenschutzmaßnahmen stehen.
- Jegliche Datenerhebung sollten auf Datenschutzmethoden beruhen wie dem „Privacy by Design“⁴ und dem „Privacy Impact Assessment“⁵ basieren.
- Spezialisierte Fachberatungsstellen für Betroffene von Menschenhandel sollten nicht gezwungen werden, die Daten ihrer Klient*innen an staatliche Instanzen oder Dritte weiterzugeben.
- Mandat und Zweck der Berichterstattungsstelle sollten auf klaren Kooperationsstandards zwischen den spezialisierte Fachberatungsstellen für Betroffene von Menschenhandel und den Berichterstattungsstellen basieren.

4 „Privacy by Design“ beinhaltet die Annahme, dass die Privatsphäre in Zukunft nicht allein durch rechtliche und regulierende Rahmenkonzepte gesichert werden kann. Der Schutz der Privatsphäre muss die Grundlage jedes organisatorischen oder institutionellen Handelns sein.

5 2009 erstellte die Europäische Kommission die Empfehlung „Commission Recommendation on the implementation of privacy and data protection principles in applications supported by radio-frequency identification“ zur Durchführung von Beurteilungen der Auswirkungen auf und Risiken für die Privatsphäre.

- Spezialisierte Fachberatungsstellen für Betroffene von Menschenhandel sollten als unabhängige Akteure agieren und dürfen von den entsprechenden staatlichen und zwischenstaatlichen Instanzen nicht als Datenlieferant*innen missbraucht werden.
- Spezialisierte Fachberatungsstellen für Betroffene von Menschenhandel sollten von Datenschutzexpert*innen geschult werden, um ihre technische Ausstattung und Datenbanken kontrollieren und unautorisiertem Zugang durch Dritte zu verhindern.
- Die Berichterstattungsstelle sollte unabhängig sein. Unabhängigkeit bedeutet hierbei nicht nur unabhängig von den gegenwärtigen staatlichen Instanzen, sondern ebenfalls unabhängig von deren entsprechenden Mandaten und/oder Interessenskonflikten.
- Die Berichterstattungsstelle sollte regelmäßig von den nationalen Datenschutzbehörden und den nationalen Überwachungsgremien für Menschenrechte geprüft werden.
- Die Berichterstattungsstelle sollte keine operative Rolle im entsprechenden nationalen Weiterleitungsmechanismus (NRMs) einnehmen.
- Die Datenerhebung durch die Berichterstattungsstelle sollte sich nicht nur auf den Menschenhandel allein beschränken, sondern auch die breiteren Rahmenbedingungen von Wirtschaftsordnung, Exklusion, Rassismus, Grenzkontrollen, Deregulierung der Arbeit etc. in Betracht ziehen.

LITERATURANGABEN ZUM VORWORT

Amnesty International (2013) *Scotland's Slaves. An Amnesty International briefing on trafficking in Scotland 2013* [Zugriff am 20. September 2013]. Siehe: <http://www2.amnesty.org.uk/resources/scotlands-slaves-amnesty-international-briefing-trafficking-scotland>.

Andrijasevic, R. (2007) 'Beautiful Dead Bodies: gender, migration and representation in anti-trafficking campaigns.' *Feminist Review* Nr. 83: 24-44.

Aradau, C. (2004) 'The Perverse Politics of Four-Letter Words: risk and pity in the securitization of human trafficking.' *Millennium: Journal of International Studies* Nr. 33 (2): 251-277.

ASTRA Anti-Trafficking Action (2013) *Human Trafficking - Manual for Journalists 2009* [Zugriff am 18. September 2013]. Siehe: <http://www.astra.org.rs/en/pdf/novinari08ENG.pdf>.

European Commission (2013) *Communication from the Commission to the European Parliament, The Council, The European Economic and Social Committee and the Committee of the Regions. The EU Strategy towards the Eradication of Trafficking in Human Beings 2012-2016* 2012 [cited 14 September 2013]. Available from http://ec.europa.eu/home-affairs/doc_centre/crime/docs/trafficking_in_human_beings_eradication-2012_2016_en.pdf.

Eurostat, and DG Home Affairs (2013) *Trafficking in Human Beings. Publications Office of the European Union 2012* [Zugriff am 20. September 2013]. Siehe: http://ec.europa.eu/anti-trafficking/EU+Policy/Report_DGHome_Eurostat.

Frontex (2013) *Situational Overview on Trafficking in Human Beings 2011* [Zugriff am 20. September 2013]. Siehe: http://frontex.europa.eu/assets/Publications/Risk_Analysis/Situational_Overview_on_Trafficking_in_Human_Beings.pdf.

ICMPD (2002) *Regional Standard for Anti-Trafficking Police Training in SEE*. Vienna, Austria: International Centre for Migration Policy Development.

- ICMPD (2007) Regional Standard for Anti-Trafficking Training for Judges and Prosecutors in SEE 2004 [Zugriff am 22. Juni 2007]. Siehe: <http://www.icmpd.org/829.html>.
- Laczko, F. (2002) ‚Human trafficking: the need for better data.‘ Migration Information Source Nr. 1.
- Laczko, F. (2007) ‚Enhancing Data Collection and Research on Trafficking in Persons.‘ In *Measuring Human Trafficking*, edited by Ernesto U. Savona and Sonia Stefanizzi, 37–44. Springer New York.
- Ogrodnik, L. (2013) *Towards the Development of a National Data Collection Framework to Measure Trafficking in Persons*. Statistics Canada, Canadian Centre for Justice Statistics 2010 [Zugriff am 14. September 2013]. Siehe: <http://odesi1.scholarsportal.info/documentation/PHIRN/YCS/85-561-m2010021-eng.pdf>.
- Rouvroy, A., and Y. Poullet (2009) ‚The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy.‘ In *Reinventing data protection?*, edited by Serge Gutwirth, Yves Poullet, Paul de Hert, Cécile de Terwangne and Sjaak Nouwt, 45–76. New York: Springer.
- Simmel, G. (1906) ‚The Sociology of Secrecy and of Secret Societies.‘ *American Journal of Sociology* Nr. 11 (4): 441–498. doi: 10.2307/2762562.
- Sullivan, S., and N. Tuana (2007) *Race and epistemologies of ignorance*: SUNY Press.
- UNODC (2013) *Anti-Human Trafficking Manual for Criminal Justice Practitioners*. UNODC, 2009a [Zugriff am 20. September 2013]. Siehe: <http://www.unodc.org/unodc/en/human-trafficking/2009/anti-human-trafficking-manual.html>.
- UNODC (2013) *Global Report on Human Trafficking*. UN.GIFT 2009b [Zugriff am 18. September 2013]. Siehe http://www.ungift.org/docs/ungift/pdf/humantrafficking/Global_Report_on_TIP.pdf.
- Warren, C., and B. Laslett (1977) ‚Privacy and Secrecy: A Conceptual Comparison.‘ *Journal of Social Issues* Nr. 33 (3): 43–51. doi: 10.1111/j.1540-4560.1977.tb01881.x.
- Wolff, K. H. (1950) *The Sociology of Georg Simmel*. New York: The Free Press.

AUSGEWÄHLTE LITERATURANGABEN

Charter of Fundamental Rights of the European Union (2000/364/01).

COM(2012)286 final, The EU Strategy towards the Eradication of Trafficking in Human Beings 2012–2016, 19 June 2012.

Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data 1981.

Council of Europe Convention on Action against Trafficking in Human Beings, Warsaw 16.V.2005.

Council of the European Union, Conclusion on Establishing an Informal EU Network of National Rapporteurs or Equivalent Mechanisms on Trafficking in Human Beings, during the 2946th Justice and Home Affairs Council meeting in Luxembourg on 4 June 2009.

Directive 95/46/EC of the European Parliament and of the Council of 24.10.1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJL 281, 23.11.1995).

Directive 2011/36/EU of the European Parliament and of the Council of 5 April 2011 on preventing and combating trafficking in human beings and protecting its victims, and replacing Council Framework Decision 2002/629/JHA.

European Agency for Fundamental Rights (FRA): Data Protection in the European Union, the role of National Data Protection Authorities. Strengthening the fundamental rights architecture in the EU II" (2010).European Convention on Human Rights (ECHR) 1950.

European Commission Impact Assessment SEC (2012) 72 final, Annex 1, http://ec.europa.eu/justice/data-protection/document/review2012/sec_2012_72_en.pdf.

European Court of Human Rights 22 October 1981, Application No. 7525/76, *Dudgean v The United Kingdom*.

European Court of Human Rights 22 October 1988, Application No. 10581/83, *Norris v. Ireland*.

European Court of Human Rights 16 December 1992, Application No. 13710/88, *Niemitz v Germany* .

European Court of Human Rights 18 October 2011, Application No. 16188/07, *Khelili v Switzerland*.

European Court of Justice, Case C-518/07, *European Commission v. Federal Republic of Germany*, Judgement of 9 March 2010.

Information Commissioner's Office: Conducting privacy impact assessments, Code of Practice, February 2014.

International Centre for Migration Policy Development (ICMPD), Guidelines for the Development of a Transnational Referral Mechanism for Trafficked Persons. South-Eastern Europe, Vienna 2009.

International Labour Organisation (ILO), A global Alliance against Force Labour, Global report under the follow-up to the ILO Declaration on Fundamental Principles and Rights at Work. Report of the Director-General 2005.

Prevent, Combat, Protect ,Human Trafficking. Joint UN Commentary on the EU Directive – A Human Rights Based Approach, November 2011.

The Hague Ministerial Declaration on European Guidelines for Effective Measures to Prevent and Combat Trafficking in Women for the Purpose of Sexual Exploitation. Ministerial Conference under the Presidency of the European Union, The Hague 24–26 April 1997.

www.dataact-project.org

© KOK e.V. 2015

KOK

Bundesweiter Koordinierungskreis
gegen Menschenhandel e.V.

www.kok-gegen-menschenhandel.de

Projektpartner:



www.lastradainternational.org