DATA PROTECTION CHALLENGES IN ANTI-TRAFFICKING POLICIES

A Practical Guide

datACT

data protection in anti-trafficking action

Data Protection Challenges in Anti-Trafficking Policies

A Practical Guide

Publisher
KOK e.V. – German NGO Network against Trafficking in Human Beings
(Bundesweiter Koordinierungskreis gegen Menschenhandel e.V.)

Authors
Pia Roth, Dr. Bärbel Heide Uhl, Marjan Wijers, Wiesje Zikkenheiner.
The authors would like to thank Marieke van Doorninck,
Ulrike Gatzke, and Tabea Richter for their useful comments.

Design and Typesetting
Kathrin Windhorst, Tim Haberstroh

Printed by
OKTOBERDRUCK AG, Berlin

The publication has been produced with the
financial support of the OAK Foundation.

Contact address
info@kok-buero.de

KOK e.V.
Kurfürstenstraße 33
10785 Berlin
Germany

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

datACT is a collaboration of KOK e.V. and La Strada International.

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

AWF	Analysis Work Files
CoE	Council of Europe
CTM	Counter-Trafficking Module
datACT	data protection in anti-trafficking action
DCIM	Data Collection and Information Management
DPA	Data Protection Authorities
EC	European Commission
ECHR	European Convention on Human Rights
ECJ	European Court of Justice
ECrtHR	European Court of Human Rights
EDPS	European Data Protection Supervisor
EEA	European Economic Association
EFTA	European Free Trade Association
EIS	Europol Information System
EU	European Union
Eurostat	Statistical Office of the European Union
ICMPD	International Centre for Policy Development
ICT	Information and Communication Technology
IGO	International Governmental Organisation
ILO	The International Labour Organisation

IOM	International Organisation for Migration
IT	Information Technology
NGO	Non Governmental Organisation
NREM	National Rapporteur or Equivalent Mechanisms
NRM	National Referral Mechanism
OSCE	Organisation for Security and Co-operation in Europe
PIA	Privacy Impact Assessment
TIP	Trafficking in Person
TRM	Transnational Referral Mechanism
UK	United Kingdom
UN	United Nations
UNODC	United Nations Office on Drug and Crimes
VVR	Dutch Association of Women and Law
Wbp	Dutch transposition of the Data Protection Directive

PROLOGUE

Human trafficking: between data and knowledge

by Dr. Claudia Aradau[1]

Human trafficking is now widely recognised as a complex issue, requiring differentiated or 'holistic' approaches as the literature names them. "The need for more effective anti-trafficking governance is connected to notions of 'limitations' or 'lack of knowledge about human trafficking."

'The need for better data' is now unanimously recognised by experts as one of the necessary steps for improving anti-trafficking strategies (Laczko 2002, 2007). It is now widely acknowledged that the data on human trafficking is insufficient, unreliable, incomparable, and limited (Ogrodnik 2010). Executive Director Antonio Maria Costa, of the United Nations Office on Drug and Crimes (UNODC), deems it a 'knowledge crisis' and goes on to explain its ramifications for anti-trafficking:

> » Only by understanding the depth, breadth and scope of the problem can we address [...] how to counter it. So far we have not attained much knowledge and therefore initiatives have been inadequate and disjointed. (UNODC 2009b)

In this was combating human trafficking, protecting victims of trafficking and preventing the phenomenon is seen to be dependent on reducing this systemic lack of knowledge. The implication is that if we could just acquire the data, we could solve the problems of human trafficking. Assumptions about the lack of data and the different understandings about what constitutes a lack of knowledge is not discussed; acquiring data is immediately supposed to lead to better action and better protective and preventive mechanisms.

1 Dr. Claudia Aradau, Reader in International Politics, King's College, London, UK, is an internationally recognised researcher on data politics. The prologue presents her keynote speech on the occasion of the international datACT conference: 'Data protection and right to privacy for marginalized groups: a new challenge in anti-trafficking policies' , which was held in Berlin, 25–27 September 2013.

In these debates, the focus has been on responses in the absence of an analysis of whether the problem of data acquisition has been soundly formulated. As any social scientist knows, asking the wrong question will not lead to any right answers, however much one could try to refine the answer. This paper addresses the question of data in human trafficking governance by placing it in the broader context of lack of knowledge. What does it mean to say that we have a problem of lack of knowledge concerning human trafficking? I argue that the lack of knowledge about human trafficking needs to be understood as threefold: ignorance, secrecy and uncertainty. Each of these understandings about the lack of knowledge entails different implications for how data is acquired, how it is deployed, and to what purposes. In each of these cases, I propose alternative ways to approach the problem of the lack of knowledge regarding human trafficking.

Ignorance: training and awareness-raising

The lack of knowledge about human trafficking has been first presented as a problem of ignorance. Ignorance appears under many guises: the ignorance of victims of trafficking about migration possibilities, about legal rights or protection possibilities or the ignorance of authorities on the phenomenon of trafficking. A Manual for Journalists in Serbia, prepared by a local anti-trafficking organisation with the support of the Organisation for Security and Co-operation in Europe (OSCE), summarises the extent and forms of ignorance:

> One of the circumstances human traffickers benefit from is the lack of knowledge, especially among young women, about actual possibilities of migration into Western European countries: they either have no or very little information about living conditions and employment opportunities in the European Union. They do not know their rights or if and how they can be issued legal working permits; they also do not know that they cannot work legally with tourist (Schengen) visa and are not aware of all the risks of working in the "black" labor market (ASTRA Anti-Trafficking Action 2009, 14).

This broad 'lack of knowledge' is seen as a main impediment to victim self-identification and therefore to effective action to combat human trafficking. Related psycho-emotional factors such as fear of the traffickers, mistrust of authorities, and/or psychological dependence on the traffickers are also ultimately founded on ideas about ignorance, for example, of the fact that the traffickers can be punished, authorities can offer protection, and that the situation they are in is exploitative.

This problem of ignorance translates into the solutions calling for awareness-raising and training.[2] Awareness-raising campaigns and extensive training modules for state authorities such as judges, policemen, and border guards have been proposed and implemented.[3] What we have here is an extensive pedagogy of human trafficking, intended to reduce ignorance across the board leading to both protective and preventive effects in the future. In training professionals to recognise victims of trafficking it should be possible to put more effective action in place. The data collected on victims of trafficking informs the training manuals and handbooks, directing experts to recognise the 'signs' of human trafficking in cases where victims themselves might be unaware of what might befall them or of the situation they are in.

However, there has been little critical reflection on the idea of ignorance informing pedagogical practices of anti-trafficking. There is an assumption that there are experts who know what counts as knowledge and ignorance. They also know who is ignorant and about what. There are at least two problems with these assumptions. First, this approach does not consider women as epistemic agents. The knowledge that victims of trafficking might have about their situation is disqualified as 'ignorance'. In so doing, it is also excluded from useful data unless it fits already existing knowledge. Second, this approach implies that ignorance is reducible through the knowledge that only some experts have. Ignorance is presented as an absence, a gap in knowledge that can be remedied through the acquisition of knowledge, instead of something that is a product of social relations between different

2 For further discussion see Andrijasevic 2007, Aradau 2004.

3 See ICMPD 2002 and 2004, UNODC 2009a.

categories of experts, or between experts and 'victims of trafficking'. The feminist scholar Nancy Tuana has coined the phrase of 'epistemologies of ignorance'[4] to capture the productive and produced function of ignorance. Ignorance and knowledge are both present, and any production of knowledge implies the production of ignorance. The question here is not about truthfulness or falsehood, but about how knowledge is rendered as illegitimate or simply not valuable. So we need to think more carefully about these assumptions of 'lack of knowledge', of ignorance when it comes to anti-trafficking strategies.

First, we need to understand knowledge as situated, rather than as lack. The assumption of ignorance renders particular voices less important or illegitimate. What would it mean to take their knowledge into consideration, as knowledge rather than ignorance, instead of assuming lack of knowledge as the starting point? Second, we also need to understand how ignorance can be strategically deployed for particular purposes. What does it mean to say that experts lack knowledge to recognise human trafficking? What if we are to take their situated knowledge as important rather than their ignorance? Finally, training and awareness-raising campaigns assume that knowledge changes what people do. Yet, these campaigns do nothing to transform the material conditions in which people live. Without an understanding of the conditions of action, learning and educational practices will continue to fail.

Secrecy: surveillance and identification mechanisms

A second important form of lack of knowledge emerges through the representation of trafficking as an underground phenomenon. For example, a 2013 Amnesty International report notes that "trafficking is an underground business and therefore it is very difficult to gain accurate information about its scale in the UK". Human trafficking is shrouded in secrecy, as it takes place in the shadows of law. Therefore, dispelling secrecy becomes a new strategy that would make anti-trafficking more effective. This entails the acquisition of

4 Sullivan and Tuana 2007.

data about secret organisations, the underground economy, or those who appear associated with these underground or shadow economies.

Yet, in so doing, there is an important shift that takes place between secrecy and privacy, with effects on all those who are in a situation of trafficking. One of the traditional understandings of the right to privacy has been that of seclusion, isolation or opacity. Warren and Laslett note in their comparison of secrecy and privacy: 'In contrast to privacy, which is simply a withdrawal from the public order, secrecy operates in disregard of or opposition to that order' (1977). Unlike privacy, which is perceived as legitimate, secrecy appears as illegitimate when applied to particular individuals or non-state groups. If privacy is the area of personal knowledge where only intimates can have access, the problematisation of secrecy in relation to knowledge renders the injunction to knowledge acquisition as an injunction to access to personal knowledge:

» From secrecy, which shades all that is profound and significant, grows the typical error according to which everything mysterious is something important and essential. Before the unknown, man's natural impulse to idealize and his natural fearfulness cooperate toward the same goal: to intensify the unknown through imagination, and to pay attention to it with an emphasis that is not usually accorded to patent reality (Wolff 1950, 333).

This approach implies that surveillance is needed in order to access this secret world and identify that people who operate in it. In the case of trafficking, dispelling secrecy trumps the protection of privacy.

In representing the unknowns of human trafficking as simply the illegitimate secret of criminal organisations, anti-trafficking strategies reduce the scope for privacy concerns. Secrecy requires much more careful analysis than we have had so far in statements about organised crime. One thing that we need to recall in these debates is that secrecy has long been a strategy of the excluded and the marginalised, indeed, a way of evading the reach of power. The sociologist Georg Simmel has shown that secrecy can be a form

of protection: "As a general proposition, the secret society emerges everywhere as correlate of despotism and of police control. It acts as protection alike of defence and of offense against the violent pressure of central powers' (Simmel 1906, 472). Moreover, Simmel cautions against the fallacy of seeing everything that is secret as important or illegitimate. Secrecy is both an element of human interaction and a particular strategy of protection for excluded groups. Just like ignorance, secrecy is produced as illegitimate in relation to different actors and groups. Secrecy is accepted when it is the prerogative of anti-trafficking experts – Frontex[5], for instance, argues that 'due to the sensitivity of risk profiles' of victims of trafficking, these should be restricted to law enforcement only (2011). Here, the production of knowledge also produces non-knowledge, as secrecy legitimates particular actors as possessors of knowledge at the expense of others. Who is allowed to keep secrets? Secrecy remains unquestioned when relations of trust underpin relations of knowledge. Effectively, secrecy is disallowed in the absence of trust. So the question of lack of knowledge and secrecy is also a question about how trust is produced and withdrawn.

Uncertainty: data collection

The third understanding of the lack of knowledge concerns uncertainty. Human trafficking is recognised to be a rapidly changing phenomenon. Therefore, the collection and processing of data is thought to offer a better understanding of the future. Data collection is not only a remedy to experts' assumed ignorance but also a remedy to the uncertain nature of the phenomenon. Protecting victims and preventing human trafficking presupposes a certain anticipatory capacity on the part of experts: how will traffickers act, what will be the victims' reactions and so on? Given the uncertainties associated with human trafficking the European Commission proposed in 'The EU Strategy towards the Eradication of Trafficking in Human Beings 2012–2016', to create a system of data collection:

5 European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union (Frontex).

» The trends, patterns and working methods of traffickers are changing in all the different forms of trafficking in human beings, adapting to changing patterns of demand and supply. Forms of exploitation are often merged and intertwined, making it hard to detect the exact form of exploitation victims are subjected to. This makes it even harder to identify victims. It is necessary to be able to understand such trends quickly and ensure an effective response (European Commission 2012).

The EU has singled out human trafficking as one of the priority areas for data collection and focused on developing 'work on methodologies and data collection methods to produce comparable statistics on trafficking in human beings' (European Commission 2012). More and better data is seen as a solution to the ineffectiveness of anti-trafficking policies. This is not simply a question of ignorance or secrecy, but a question of uncertainty. There is uncertainty about new methods that traffickers might use, about new routes, new victims, and new forms of exploitation. A different preventive logic is at work here. You don't prevent by reducing ignorance or dispelling secrecy, but by managing uncertainty through data collection.

There is not much in the EU Commission documents as mentioned above about the acquisition and processing of this data. As indicated in a report by Eurostat[6], this would imply the conversion of uncertainty into risk though statistical reasoning (2012). Historically, one of the solutions to uncertainty has been that of risk probability calculations, the creation of risk profiles, and assigning risk. It uses the individual data to create new categories and profiles, without making the supporting logic visible. This means individuals cannot contest this logic because it is not available to them.

Concerns about data protection have been raised particularly in relation to data collection. I would like to end by making a couple of points about data protection. Data protection is an important right, but unfortunately it doesn't address the problems of statistical knowledge and risk profiling in response

6 Eurostat is the statistical office of the European Union.

to uncertainty. By displacing the individual through categories of risk, data collection also makes the claim for data protection inoperative. While the various categories of data might appear helpful for our knowledge about human trafficking, and largely inoffensive in terms of privacy rights, it is not data that is the problem, but rather the way it is processed and subsequently put to use by the various agencies involved. If you are a citizen of one of the assumed countries of origin, what implications does this have for your freedom of movement when you encounter consular or border authorities? As Antoinette Rouvroy and Yves Poullet have argued:

> [V]ast collections and intensive processing of data enable data controllers such as governmental authorities or private companies to take decisions about individual subjects on the basis of these collected and processed personal information without allowing for any possibility for the data subjects to know exactly which data would be used, for which purposes, for which duration and overall without control of the necessity of these proceedings in consideration of the purposes pursued by the public or private bureaucracies (Rouvroy and Poullet 2009, 68–69).

So, to end, it seems to me that the challenges in relation to anti-trafficking concern how to know responsibly rather than simply the postulation of knowledge at all costs, and in particular, how to know in ways that are not destructive of freedom and human dignity. One path I suggested is to start from knowledge as situated and analyse the ways in which this knowledge might be ignored or rendered uncertain. Secondly, we need to get rid of the fantasy that there is such a thing as 'raw' data that will give us an understanding of how to act on the future, how to prevent human trafficking from reoccurring or happening. There is no such thing as raw data, nor is there any such thing as innocent data. Moreover, human rights have only limited efficacy against the logic of statistical data processing and preventive risk management. What is important is to make the ways of reasoning about data visible – dispel the secrecy in processing of data in order to create conditions for the exercise of human rights.

To conclude, knowing responsibly implies analysing what forms of 'lack of knowledge' the agencies involved in human trafficking create themselves. What forms of ignorance, secrecy, and/or uncertainty emerge in this very process, for example, about how the data is used by border agents, or uncertainty around how individuals would be treated. These are not solved through more knowledge but through creating trust and empathy. Knowing more is, after all, neither knowing nor acting better.

1. INTRODUCTION

The rights-based gathering and analysis of data on trafficking in persons is an important instrument for increasing knowledge and for monitoring trends and patterns at the national, regional and international level. In addition, data gathering and analysis help to set baselines against which Member States can assess progress in the implementation of national policies, strategies and programs.

Trafficking in persons is a crime that is often committed across borders and therefore requires Member States to cooperate and coordinate among themselves as well as with international and regional organisations. In order to improve international cooperation and coordination, formal and informal cooperation is promoted, such as establishing communications procedures, and information and data exchange.

This requires significant processing of data, in many cases it involves personal data. Consequently, it may lead to a risk of intrusion into the privacy of trafficked persons, potentially violating their right to respect for private and family life (Art. 8 European Convention Human Rights), and risks the abuse of personal data. Therefore, the collection of data for developing effective actions to combat trafficking cannot be put in place without a solid data protection scheme.

More importantly, data on trafficked persons are not only collected in the framework of police and justice cooperation in criminal matters and the organisation of national and transnational assistance, but also for other requirements and purposes carried out by national governments, intergovernmental organisations (IGOs), non-governmental organisations (NGOs) and private businesses. While data collection often serves the commercial interests of private companies, civil society organisations offering service provision often face multiple requirements to collect personal data of trafficked persons. On the one hand, they are obliged by (governmental) donors to provide quantitative information documenting the social work, while on the other hand their clients must be registered into the existing social welfare and health systems

in order to access financial and other support available to trafficked persons; both require the collection and storage of personal data, including registration in social welfare systems, return programs, or use of cloud computing services.

Some National Rapporteur or Equivalent Mechanisms (NREMs) in Europe collect only non-personal/anonymised data from victims of trafficking, others again focus on retrieving personalised data from victims (and their families), including details of their experiences of violence, and information about the (suspected) offenders.

While politics on anti-terror measures focus on perpetrators, anti-trafficking politics generally aim to 'profile' potential and presumed victims of trafficking. When it comes to data collection this victim-centred approach – a term often used as a synonym for a human rights based approach – falls into a different, more restrictive perspective. International and intergovernmental organisations have developed guidelines and tools for data collection with a strong focus on collecting victim data.[7]

The risks attached to the collection, exchange, and various forms of data processing of victim's personal data raise serious concerns for their privacy and safety. The protection of victims' private life and identity is not only essential for their physical safety, given the risk of retaliation from their traffickers, but also in view of potential stigmatization impacting on the possibility of rebuilding a life in their country of origin or destination.

There are additional risks for victims of trafficking for prostitution who may also face reprisals from authorities. In many countries, in particular (South) Eastern European countries, working in the sex industry is a criminal or public order offence. Victims of trafficking for prostitution risk arrest, prosecution, and/or punishment. Moreoever, people who have been trafficked into forced criminal activities may be exposed to prosecution and social stigmatization once their personal data has been shared among authorities and other stakeholders.

7 See data collection instruments designed by ICMPD and IOM in chapter 5; and the 'DNA, human right and human trafficking programme' of the Duke University at http://kenan.ethics.duke.edu/humanrights/dna-human-rights-human-trafficking-sep-13-2/.

Furthermore, alerting to the involvement of state officials in trafficking should be taken into account, raising the issue of corruption and ensuing risk of abuse of data. At the same time, it is crucial for victims' access to assistance that they can trust assistance providers to keep their information fully confidential.

It is therefore paramount that all data collection and processing mechanisms should protect the rights of trafficked persons as data subjects. The term 'trafficked person' as used in this publication includes crime victims exploited in all economic sectors, including sex work, domestic work, agriculture, construction work, food industry, and care taking.

The practical guide will explore the implications and dimensions of data protection in anti-trafficking politics. In a first step, we provide a general overview of European data protection legal instruments, followed by a detailed discussion on the application of the concept on 'sensitive data'. In a second step, we discuss the specific instruments on data and privacy within the anti-trafficking policy framework. Finally, we explore the possibilities to break down existing legal and political principles into concrete measures for practitioners in the non-governmental, governmental and inter-governmental sector.

2. MAIN DATA PROTECTION INSTRUMENTS

This chapter provides an overview of European data protection laws and discusses its implications.

The basis for all European data protection instruments is **Article 8 of the 1950 European Convention on Human Rights** (ECHR): the right to respect for private and family life. Article 8 prevents public authorities from interfering with the private life of citizens unless certain conditions have been met. Under the EU Charter of Fundamental Rights (2009[8]) the protection of personal data is considered an autonomous fundamental right, next to the right to privacy.

The two main instruments in the area of data protection are:

1. Directive 95/46/EC[9] (hereafter **Data Protection Directive)** is the centrepiece of legislation on data protection in EU law. The definitions and principles within the Directive are the main reference for data protection provisions in other instruments. All EU countries are required to implement this Directive in national legislation. However, data processing activities in the area of police and judicial cooperation in criminal matters are excluded.[10]

2. Given the limited scope of the Data Protection Directive, from 1993 until 2009 the main reference governing police and judicial cooperation was the 1981 Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (hereafter **CoE Convention 108)**. In 2008, a separate Framework Decision (2008/977/HA) was adopted, however, this only pertains to cross-border data processing. The Council of Europe (CoE) Convention is still the

8 The Charter was proclaimed in 2000 but only got full legal effect in 2009 following the entry into force of the Treaty of Lisbon.

9 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 (OJ L 281, 23.11.1995).

10 Art 3(2) : This Directive shall not apply to the processing of personal data: [...] and in any case to processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law.

main instrument governing the processing of domestic data in criminal matters. Furthermore, the CoE Convention covers more countries than the EU Data Protection Directive.

The two key concepts in both instruments are 'personal data' and 'processing of personal data´:

'personal data' means any information relating to an identified or identifiable individual ('data subject'). Data is considered personal when it enables anyone to link information to a specific person, even if the person or body holding the data cannot make that link. That means any information that identifies or can lead to the identification of one person (data subject) from the rest of persons falls under personal data.

'processing of personal data' ('processing') means any operation which is performed upon personal data, including collection, recording, storage, retrieval, consultation, use, transmission, dissemination or otherwise making available, blocking, erasure or destruction.

EU Data Protection Directive, 1995

The purpose of data protection is to protect the individual about whom data are processed. This is achieved through a combination of rights for the individual (called 'data subject' in data protection language) and obligations for those who process data (the 'data processor') or exercise control over such processing (the 'data controller'). **Directive 95/46/EC** defines the conditions under which personal data may be processed. It was adopted in 1995 with two objectives in mind:

- to protect the right to privacy with respect to the processing of personal data,
- to guarantee the free flow of personal data between Member States.

The Directive sets the data protection standards for all EU legislative acts. It encompasses all key elements of the European Convention on Human

Rights,[11] especially Article 8, respect for private and family life. It applies to both public and private sectors, such as NGOs, IGOs and businesses, including international businesses whenever the data controller uses equipment located within the EU to process data. However, it does not cover the area of police and judicial cooperation in criminal matters.

The Directive does not impose obligations directly on people or businesses.[12] Instead, it requires that each EU Member State enacts laws to govern the processing of personal data satisfying certain minimum standards as laid down in the Directive.[13] All EU Member States have transposed the Directive. It also requires States to establish national Data Protection Authorities (DPA).

Article 29 of the Directive sets up a Working Party, an expert body composed of representatives from the Data Protection Authorities of the Member States, the EU institutions and bodies and the Commission. It has advisory status and acts independently.[14]

Principles on Data protection

- **Purpose:** data should only be used for the purposes stated and not for any other purposes;
- **Consent:** personal data should not be disclosed or shared with third parties without the data subject's consent;
- **Security:** collected data should be kept safe and secure from potential abuse, theft or loss;
- **Notice:** data subjects should be informed as to who is collecting their data;
- **Disclosure:** subjects whose personal data is being collected should be informed as to the party or parties collecting such data;

11 Recital 1 Directive 95/46/EC.

12 EU Directives are addressed to the Member States, and in principle are not legally binding for citizens. The Member States must transpose Directives into national law.

13 Recital 69, article 5 Directive 95/46/EC.

14 For more information on its activities see http://ec.europa.eu/justice/policies/privacy/workinggroup/index_en.htm.

- **Access:** data subjects should be allowed to access their data and to correct any inaccurate data;
- **Accountability:** data subjects should be able to hold data collectors accountable for following the above principles.

The Directive is grounded on seven principles, aiming to achieve harmonisation throughout the EU.[15] In short, these principles hold that personal data should not be used without the knowledge or unambiguous informed consent of the person; that they should be correct, relevant and not excessive in relation to the purpose for which they are being stored; and that the use of data, which includes disclosure, should be carried out in an accurate way. This approach based on principles allows Member States to implement the necessary measures, while taking into account local context and cultural sensitivities as well as the needs of specific sectors.

Overview of relevant provisions

Below we will discuss some of the relevant provisions of the Data Protection Directive in more detail. First, we discuss the principles and conditions for processing data, as well as the scope and limitations of the Directive. We will then pay particular attention to the category of sensitive data and examine whether or not data on trafficked person fall within this category, especially where it concerns people trafficked for or within the sex industry.

Principles and conditions for processing data

Article 6 of the Data Protection Directive lists a number of principles relating to the quality of data, whereas article 7 provides the conditions under which personal data may be processed. Article 6 further mandates that the body

15 European Commission Impact Assessment SEC (2012)72 final, Annex 1, p. 9; http://ec.europa.eu/justice/data-protection/document/review2012/sec_2012_72_en.pdf.

which determines the purposes and means of the processing of personal data, the data controller, should ensure compliance with these principles.

Article 6 Data Protection Directive – Principles relating to data quality

1. Member States shall provide that personal data must be:
   a) processed fairly and lawfully;
   b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards;
   c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;
   d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified;
   e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use.
2. It shall be for the controller to ensure that paragraph 1 is complied with.

Purpose

The first data collection principle is that data should only be used for the purpose for which it is collected (art. 6(1)(b)). This means that the reasons for which a person's data are collected, stored, shared, etc. must be:

- **Specific:** this is also needed to assess its lawfulness;
- **Explicit:** the reason has to be made clear and openly stated, also in order to allow the individual to be aware of the activities performed on his/her data and to enforce the applicable privacy rights;
- **Legitimate:** this is in line with the principle of lawfulness, meaning that the controller must have a legitimate motive to process personal data.

The respective purposes of data processing must be defined *prior* to the procedure. In addition, personal data cannot be processed for reasons that are incompatible with the ones for which they were originally collected.

Enshrined within the **principle of purpose limitation** is the **data quality principle**, which imposes the requirement that the data processed must be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed (art. 6(1)(c)). This relates to the so-called **data storage principle** which holds that one may only use the amount of data that is necessary for the specified legitimate purpose (art. 6(1)(e)). This principle has given rise to various discussions on whether personal data has an 'expiration date' or whether data may be kept forever. Assuming that the purpose for which data are relevant still exists, personal data may be kept. Subsequently, when the processing purpose is fulfilled, personal data should be erased, made anonymous or used for a different legitimate purpose.

The data quality principle further provides that personal data must be accurate and, where necessary, kept up to date. This puts an obligation on the data controller to take every reasonable step to guarantee that personal data which are inaccurate or incomplete are erased or rectified, having regard to the purposes for which they were collected or for which they are further processed (art. 6(1)(d)). The reason behind this is that incomplete, inaccurate or wrong information may cause significant damage to the person concerned.

Consent

'Consent' is a key concept within the Directive and is defined as "any freely given, specific, and informed indication" of the person's wish to agree with the processing of her or his personal data. Moreover, consent has to be given "unambiguously".[16] For consent to be unambiguous, the procedure for obtaining and providing consent must leave no doubt as to the person's intention. The notion of consent is founded on the idea that the individual should be in control of how their personal data is being used. Article 7 of the Data Protection Directive lists the criteria for data processing:

Article 7 Data Protection Directive – Criteria for making data processing legitimate

Member States shall provide that personal data may be processed only if:

a) the data subject has unambiguously given his consent; or

b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or

c) processing is necessary for compliance with a legal obligation to which the controller is subject; or

d) processing is necessary in order to protect the vital interests of the data subject; or

e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or

f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1 (1).

16 Articles 2(h) and 7(a) Data Protection Directive.

However, Member States currently interpret these criteria differently, ranging from a general requirement to obtain written consent to allowing for the acceptance of implicit consent. Furthermore, the 2012 EC Assessment on personal data protection indicates that national DPAs apply different interpretations of consent.[17] As a consequence what constitutes valid consent in one Member State may not be legally valid in others.[18]

According to Opinion 15/2011 of the Working Party on the definition of consent:

> Consent can only be valid if the data subject is able to exercise a real choice, and there is no risk of deception, intimidation, coercion or significant negative consequences if he/she does not consent. If the consequences of consenting undermine individuals' freedom of choice, consent would not be free.[19]

For example, in the case where someone is in a situation of dependency on the data controller because of the nature of the relationship or other special circumstances, and providing data is a precondition to subsequent actions, they may fear being treated differently if they do not consent.

The Working Party goes into more detail, stating that consent must be:

> [A] voluntary decision, by an individual in possession of all of his faculties, taken in the absence of coercion of any kind, be it social, financial, psychological or other.[20]

While the latter was specifically considered in the context of consent given under the threat of non-treatment or lower quality treatment in a medical situation, this could very well extend to the provision of other services, such as psycho-

17 European Commission Impact Assessment.

18 European Commission Impact Assessment, Annex 1, p. 13.

19 Article 29 Data Protection Working Party "Opinion 15/2011 on the definition of consent", 13 July 2011, p. 12; http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf.

20 Article 29 Working Party (WP131) "Opinion on the definition of consent", p. 13.

logical, social or legal assistance. For example, consent cannot be considered freely given in cases where trafficked persons have to consent to the exchange of their personal data with third parties in order to access assistance services.

Although the timeframe for seeking consent is not explicitly defined in the Directive, there is a clearly implied general rule that consent must be given before the processing starts.[21] When there is no consent, personal data may only be processed if this is *necessary* for one of the objectives specified in article 7. This means that either the person should have consented to the processing of his or her personal data, or such processing must meet the criterion of "necessity".

Security

Confidentiality and security precautions are meant to protect personal data while stored as well as when transferred, or otherwise made accessible to third parties and regardless of whether the data is in paper and/or electronic form. There are two categories of security measures: technical and organizational. The first generally refers to measures designed to keep data secure when electronic devices and equipment are involved, (firewalls, antivirus software, authentication and authorization systems). The latter refers to instructions, policies, and internal procedures governing how personal data are handled by the data controller. Due to their nature and potential harm to the individual, sensitive data requires greater protection; in this case additional legal, organizational and technical safeguards should be considered.[22]

Chapter IV of the Data Protection Directive deals with the requirements for sending personal data outside Europe. The core provision is clear: no data should go to a third country unless that country ensures "an adequate level of protection" (art. 25(1)). In order to assess what constitutes an "adequate level of protection" the Commission takes into account the following factors:

21 Article 29 Working Party "Opinion on the definition of consent", p. 9.

22 Article 29 Working Party "Advice paper on special categories of data (sensitive data)", p. 11.

- the nature of the data;
- the purpose and duration of the proposed processing operations;
- the country of origin and of final destination;
- the legal rules in the third country, both in general and in regard to data protection; and
- the professional rules and security measures in place (art. 25(2)).

Notice and Disclosure

Personal data should be processed fairly and lawfully. 'Fairness' means that the person concerned should get reliable information on the processing of his or her personal data. The data controller is responsible to provide information to the person whose data is processed as well as the supervisory authority. This applies both when personal information is collected directly from the person and when obtained otherwise.

Notice to the individual

Transparency is widely regarded as a core principle regarding processing personal data. The right of a 'data subject' to information is mirrored by the obligation of the controller to provide certain mandatory information to the person concerned. According to article 10 and 11 of the Directive, this information should include the identity of the controller, the purpose of the processing, the recipients or categories of recipients of the data, whether providing information is obligatory or voluntary (including an explanation of the consequences of failure to provide the information), the right to access to personal data and to correct them, and any further information "in so far as such further information is necessary" (art. 10). When personal data are collected from third parties rather than directly from the individual, the person concerned should be informed by the data controller at the moment their personal data is recorded. In the event that the controller intends to share personal data with third parties, information should be given to the individual prior to doing so (art. 11(1)).

There are a number of exemptions to the obligation to inform, for example, when compliance with this obligation is impossible or requires a disproportionate effort for the controller, or when the recording or disclosure of personal data is necessary to comply with a specific and applicable provision of law (art. 11(2)).

Notice to the supervisory authority

Except where national law provides an exemption, controllers must provide the relevant DPA with the following information prior to any processing operation (art. 18 and 19):

- the name and address of the controller;
- the purpose(s) of the processing;
- a description of the category or categories of persons affected, and of the data relating to them;
- the (categories of) recipients to whom the data may be disclosed;
- any proposed transfers to third countries; and
- a general description of the measures taken to ensure the security of processing.

The DPA should keep a register of the processing operations of which it is notified. This register must be made available for inspection by any person (art. 21). This provision aims at guaranteeing transparency of the data processing activities carried out within a Member State. In addition, it gives individuals the possibility to be informed and to enforce their privacy rights under the applicable data protection legislation.

Access to personal data

The right of access enables individuals to supervise the processing of their personal data. According to article 12 of the Directive, they have the right to obtain information as to whether or not their personal data is being pro-

cessed, the purpose of such processing, the source and content of the data concerned, and to whom the data are disclosed. They also have the right to correct, erase, or block the transfer of inaccurate or incomplete data. Moreover, it must be made possible to exercise one's privacy rights in an easy manner without constraints, at reasonable intervals of time, and without excessive delays or expenses. In addition, individuals have the right to object at any time to the processing of data relating to them (art. 14(a)).

The right to access, to correct and to object are expressed in general terms and do not specify the ways in which individuals can actually exercise these rights. Nor does the Directive impose any deadlines for responding to requests by data subjects or offer any indication or guidelines for fees that may be requested relating to the rectification, erasure and blocking of personal data.[23] Article 13 defines the circumstances under which the data subject's rights may be exempted or restricted, notably to safeguard national security, national defence, public security, the prosecution of criminal offences, an important economic or financial interest of a Member State or of the European Union, or for the protection of the data subject or the rights and freedoms of others.

Accountability

As mentioned above, the Directive requires each Member State to set up a supervisory authority in the form of an independent Data Protection Authority (DPA) to monitor the application of its data protection law (art. 28). The European Court of Justice (ECJ) has clarified the understanding of 'independent' in relation to DPAs as incompatible with being subject to State oversight.[24] Supervisory authorities must be endowed with investigative powers as well as effective powers of intervention, such as powers to order blocking, erasure or destruction of data, or to impose a temporary or permanent ban on processing (art. 28(3)).

23 European Commission Impact Assessment, Annex 2, p. 32.

24 ECJ, Case C-518/07, European Commission v. Federal Republic of Germany, Judgment of 9 March 2010.

Right to be forgotten

The right to be forgotten refers to the right of any person to have their data no longer processed and deleted when they are not needed anymore for the original purpose or another legitimate purpose. It is indirectly supported by the current Data Protection Directive which requires data controllers to delete personal data when they are no longer required for legitimate purposes (art. 6).

The Directive also provides for an active enforcement mechanism granting individuals the right to request information from the data controller regarding if and which personal data are being processed in relation to them. Also, an individual can demand the rectification, erasure or blocking of data in cases where, for example, the information is no longer accurate, he or she withdraws their consent, or because the period of reasonable storage has been exceeded (art. 12). In practice, however, it is difficult for an individual to enforce this right.

Policy debates argue for a more prominent and explicit right to be forgotten. Such a right has indeed been included in the proposed reform of the current legal framework on data protection.[25]

Scope of application

Article 1(1) of the Data Protection Directive explains the scope of application:

> In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons and in particular their right to privacy with respect to the processing of personal data.

25 In 2012 the Commission adopted a package for reforming the European data protection framework including a proposal for a new Regulation (COM(2012)11 final) and Directive (COM(2012)10 final).

The Directive applies to natural persons, that is, to human beings. The right to protection of personal data is universal and not restricted to nationals or legal residents of a certain country.[26] Recital 2 of the Data Protection Directive is explicit on this point, stating that: "[D]ata processing systems are designed to serve man" and "must, whatever the nationality or residence of natural persons, respect their fundamental rights and freedoms".[27]

Member States' legislation outlines more precisely the concept of personality, understood as the capacity to be the subject of legal relations, starting with the birth of the individual and ending with his death. Personal data are therefore data relating to identified or identifiable *living* individuals. Thus, the Directive is in principle not applicable to information related to individuals who are no longer living.[28]

The Directive governs electronic (digital) data, as well as written and oral communications. It applies to data processed both by automated means, such as a digitised customer database, as well as by manual systems, for example, where the data forms part of a paper filing system or are intended to form part of such system.[29]

A number of provisions contain a degree of flexibility, intended to strike a balance between protection of the individual's rights and the legitimate interests of data controllers, third parties and the public interest.[30]

26 Article 29 Working Party "Opinion on the concept of personal data", p. 21, ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf.

27 Directive 95/46/EC , Recital (2).

28 Article 29 Working Party "Opinion on the concept of personal data", p. 22. However, according to the Working Party, the data of deceased may still indirectly receive protection in certain cases, e.g. when it is not possible for the data controller to ascertain whether the person to whom the data relate is still living or dead, or in cases where the information on dead individuals may also refer to living persons (e.g. medical conditions). Information on deceased persons may be subject to specific protection granted by sets of rules other than data protection legislation, e.g. the obligation of confidentiality of medical staff does not end with the death of the patient.

29 Article 3(1) Data Protection Directive. For example, the traditional paper files, such as a card file with details of clients.

30 Article 29 Working Party Opinion on the concept of personal data, p.5.

International organisations

The Directive applies to the public and private sectors, including non-governmental organisations (NGOs), intergovernmental organisations (IGOs) and businesses.[31] In addition, the provisions apply to data controllers operating within the EU, and to international data controllers using equipment located inside the EU for processing personal data. This is particularly relevant for international businesses and organisations owning or using computing centres located within the European Community; they must comply with the laws of the Member State(s) concerned and thus indirectly with the Directive.

However, one of the problems related to cross-border data processing identified by the European Commission in its Communication on "A comprehensive strategy on data protection in the European Union" (2010) is the lack of clarity around jurisdiction. It is not always clear to either data controllers and DPAs which Member State is responsible and which laws are applicable when several Member States are involved. For example, when a multinational is established in different Member States, or when the data controller is not established in the EU but provides its services to EU residents.[32]

Limitations

The Data Protection Directive does not apply in two contexts:

- when activities are outside the scope of EU law. This includes "processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing

31 European Commission Impact Assessment, Annex 1, p. 10.

32 European Commission Communication on "A comprehensive strategy on data protection in the European Union", Brussels, p. 11. As reasons for the Communication the Commission indicates inter alia the increased risks to privacy and the protection of personal data associated with online activities (think e.g. of social networking sites and cloud computing) and the fact that the means of collecting of personal data has become increasingly sophisticated and less easily detectable (COM(2010)XXX final). http://www.statewatch.org/news/2010/oct/eu-com-draft-communication-data-protection.pdf.

operation relates to State security matters) and the activities of the State in areas of criminal law"[33].

- When the data processing is a "purely personal or household activity"[34]. For example, such activities as creating a digital spread sheet of names and addresses for mailing birthday party invitations or graduation announcements.

In addition, Member States are required to provide exemptions for "processing carried out solely for journalistic purposes", and where necessary to reconcile freedom of "artistic or literary expression" with privacy.[35]

Third countries

An important feature of the Directive is the restrictions it places on the transfer of personal data to countries outside the EU in order to counteract data processing operations being moved outside of the EU to avoid compliance with its rules. Article 25(1) of the Data Protection Directive states:

> The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if [...] the third country in question ensures an adequate level of protection.[36]

Transfers to countries that do not meet the criteria for ensuring an adequate level of protection are only allowed after the originating party takes additional measures to ensure that the data is adequately protected abroad. The DPAs of the EU Member States have the final authority to forbid or permit transfers.[37]

33 Article 3(2) Data Protection Directive.

34 Ibid.

35 Article 9 Data Protection Directive.

36 Updated decisions on adequacy findings are published at http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm.

37 Article 26(2) Data Protection Directive.

Sanctions

The Directive ensures compliance with its rules through procedural provisions on liabilities, sanctions, judicial remedies, and supervisory authorities.[38] Violations may implicate two levels of liability:

First, violations may result in sanctions set out by the National DPA or a judicial authority. The Directive requires that each Member State establishes sanctions for the infringement of its provisions.[39] These sanctions may take the form of fines and/or imprisonment. Second, violations may result in civil liability to the individual whose rights are violated. The Directive requires that:

> » Member States provide that any person who has suffered damage as a result of an unlawful processing operation or of any act incompatible with the national provisions adopted pursuant to this Directive is entitled to receive compensation from the controller for the damage suffered.[40]

However, the legal system of various Member States effectively rules out the possibility of successfully seeking compensation for a violation of data protection rights. Barriers include factors like the burden of proof, difficulties in the quantification of damages and a lack of support from the supervisory bodies.[41]

Sensitive data

Particularly interesting in relation to trafficked persons is the category of 'sensitive data'. Both CoE Convention 108 and the Data Protection Directive are based on the premise that certain categories of personal data present a greater risk to a person's private life than 'regular' personal data and

38 Chapter III of the Data Protection Directive.

39 Article 24 Data Protection Directive.

40 Article 23(1) Data Protection Directive.

41 European Union 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), p. 8; http://fra.europa.eu/sites/default/files/fra_uploads/815-Data-protection_en.pdf.

therefore require extra protection. Processing such data is subject to more stringent restrictions. Article 8(1) of the Directive defines sensitive data as:

» [D]ata revealing racial or *ethnic origin*, political opinions, religious or philosophical beliefs, trade union membership, and the processing of data concerning *health* or *sex life*.

As a general rule the processing of sensitive data is prohibited, with limited exceptions under certain circumstances and safeguards. For example, an exception might be for medical reasons or the processing of data of its members by an association or trade union.

Art. 8 Data Protection Directive – Sensitive data

1. Member States shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.
2. Paragraph 1 shall not apply where:
   a) the data subject has given his explicit consent to the processing of those data; or
   b) processing is necessary for the purposes of carrying out the obligations and specific rights of the controller in the field of employment law in so far as it is authorized by national law providing for adequate safeguards; or
   c) processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his consent; or
   d) processing is carried out in the course of its legitimate activities with appropriate guarantees by a foundation, association or any other non-profit-seeking body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members of the body or to persons who have regular contact with it in connection with its purposes and that the data are not disclosed to a third party without the consent of the data subjects; or

e) the processing relates to data which are manifestly made public by the data subject or is necessary for the establishment, exercise or defence of legal claims.

3. Paragraph 1 shall not apply where processing of the data is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those data are processed by a health professional subject under national law or rules established by national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy.
4. Subject to the provision of suitable safeguards, Member States may, for reasons of substantial public interest, lay down exemptions in addition to those laid down in paragraph 2 either by national law or by decision of the supervisory authority.
5. Processing of data relating to offences, criminal convictions or security measures may be carried out only under the control of official authority or of suitable safeguards provided under national law [...].

If none of the exceptions listed in article 8 apply and the person concerned has not given his or her freely given, specific and informed consent, an exception on the prohibition of processing sensitive data is only justified when:

- it has a legal basis;
- is necessary for reasons of substantial public interest; and
- is subject to suitable safeguards.

As previously stated, the concept of personal data should be broadly interpreted and includes any data relating to an identified or identifiable individual. Personal data can be directly or indirectly sensitive. An example of directly sensitive data may be a register in which the ethnic background of a person is registered. Indirectly sensitive data is data that is not directly related to one of the categories of sensitive data, but by which sensitive information can be deduced from the context of the recorded information, for example, the records of a church community listing the names and addresses of its members. These as such do not constitute sensitive data,

but within the context of a church they indirectly reveal data about the religious belief of the persons concerned.

Does the concept of 'sensitive data' apply to data on trafficked persons?[42]

The interesting question is, of course, whether data on trafficked persons fall within the category of 'sensitive data', as defined by the Data Protection Directive. This is especially important given the increasing focus on data collection not only of offenders but also of (presumed) victims. Moreover, under the influence of harmonising data collection procedures in the EU and the OSCE region, streamlining cross-border assistance of trafficked persons, the development of transnational referral mechanisms and increasing cross-border police cooperation, personal data of trafficked persons are stored by a growing range of governmental, intergovernemental and non-governmental organisations.

In many cases this regards sensitive personal data which may expose the trafficked person to the risk of retaliation by their traffickers, prosecution or punishment by the authorities in countries where prostitutes are criminalised, and possible social exclusion. This makes the question as to whether or not data on trafficked persons should be qualified as sensitive data highly relevant.

The concept of 'sex life'

Considering the sensitive data listed under Article 8(1), it is obvious that the category of data concerning a person's sex life may be very well applicable to data on persons trafficked for the sex industry. This raises the question what must be understood under 'sex life' in the sense of article

42 The chapter on sensitive data is based on legal research carried out by Van der Feltz advocaten (W. I. Koelewijn & R. L. de Graaff), at the request of the Dutch Association of Women and Law. The research examined the compatibility of the 2009 proposed legislation reform, calling for mandatory registration of sex workers, with the Data Protection Directive and its implementation under Dutch law (Wet bescherming persoonsgegevens (Wpb)).

8(1) of the Directive. The concept of 'sex life' is not defined or explained in the Directive. Neither is there jurisprudence of the EU Court of Justice (ECJ) providing for the interpretation of the concept. The jurisprudence of the European Court of Human Rights (ECrtHR), however, does provide some guidelines. The ECrtHR has judged in several cases that sexuality is part of the most intimate aspects of an individual's privacy, meaning that only especially serious reasons can justify interference by the government.[43] In countries where prostitution is recognised as work it could be argued that data on the fact that a person works or worked in prostitution cannot be considered as data on a person's 'sex life', as it refers to a person's professional sex life and not to his or her private sexual preferences or sexual orientation.[44]

However, such a distinction between a person's professional and private life is not supported by either ECJ or ECrtHR jurisprudence. In this respect the ECJ follows the case law of the ECrtHR:

> » It is of no relevance in this respect that the data published concerns activities of a professional nature [...]. The European Court of Human Rights has held on this point, with reference to the interpretation of Article 8 of the Convention, that the term 'private life' must not be interpreted restrictively and that 'there is no reason of principle to justify excluding activities of a professional nature from the notion of 'private life' (Schecke & Eifert).[45]

The ECrtHR has always interpreted the notion of "private life" in a broad way. An example is the case *Niemietz v. Germany*, in which the ECrtHR clearly sets out this line:

43 ECrtHR 22 October 1981, Application no. 7525/76, Dudgeon v. The United Kingdom; ECrtHR 22 October 1988, Application No. 10581/83, Norris v. Ireland.

44 This reasoning would, of course, be even more questionable in the case of persons forced into prostitution against their will.

45 EU Court of Justice, C-92/09 and C93/09 of 9 November 2010 (Schecke & Eifert), § 59; see also see also EU Court of Justice, C-456/00, Österreichischer Rundfunk and Others, §§ 73 and 74; EU Court of Justice, 8 November 2007, T-194/04, Bavarian Lager Co. Ltd; and ECrtHR 16 December 1992, Application No. 13710/88, Niemietz v. Germany, § 29.

» There appears [...] to be no reason of principle why this understanding of the notion of "private life" should be taken to exclude activities of a professional or business nature since it is, after all, in the course of their working lives that the majority of people have a significant, if not the greatest, opportunity of developing relationships with the outside world. This view is supported by the fact that [...] it is not always possible to distinguish clearly which of an individual's activities form part of his professional or business life and which do not. Thus, especially in the case of a person exercising a liberal profession, his work in that context may form part and parcel of his life to such a degree that it becomes impossible to know in what capacity he is acting at a given moment of time.

To deny the protection of Article 8 on the ground that the measure complained of related only to professional activities – as the Government suggested should be done in the present case – could moreover lead to an inequality of treatment, in that such protection would remain available to a person whose professional and non-professional activities were so intermingled that there was no means of distinguishing between them.[46]

It must therefore be concluded that the distinction between one's professional and personal sexual life is at odds with the case law of the EU Court of Justice and the ECrtHR. Both courts see no reason for such distinction between professional and personal activities, especially not when they are strongly interwoven. It follows that both one's personal and professional sex life should be understood as falling within the meaning of 'sex life' under article 8(1) of the Directive. On the question as to whether or not something constitutes an infringement of privacy, the fact that it concerns a person's professional life is therefore irrelevant.

This also bears on the issue of (mandatory) registration of sex workers implemented in some EU Member States. Particular relevant in this context is

46 ECrtHR, 16 December 1992, Application No. 13710/88, Niemietz v. Germany, § 29.

the judgement of the ECrtHR in the case of *Khelili v. Switzerland*, in which it held that registering the plaintiff, a French woman, as a "prostitute" and maintaining this data in the Geneva police database for 15 years constituted a violation of her right to respect for private and family life under article 8 of the ECHR:

» In the present case, the court assesses that the storage of data about the plaintiff concerning her working life, which is part of her private life, contradicts Article 8 of the Convention, because it concerns personal data of an identified or identifiable individual. Even though the term "prostitute" was deleted from the police databank and replaced by the term "seamstress", it nonetheless survived in the data on numerous cases before the courts of the Canton of Geneva.[47]

An additional factor in this case was the court's finding that the allegation of unlawful prostitution appeared to be too vague and general, and was not supported by concrete facts. Further, Ms. Khelili had never been convicted of 'unlawful prostitution' under Swiss law.

Conditions for making an exception on the general prohibition on the processing of sensitive data

According to article 8(4) the processing of sensitive data is subject to a stricter regime. It must be:

- necessary for reasons of substantial public interest;
- subject to the provision of suitable safeguards; and
- have a legal basis.[48]

47 ECrtHR of 18 October 2011, Application No 16188/07, Khelili v. Switzerland, § 56 (only available in French). See for the press release (in English and French) http://hudoc.echr.coe.int/sites/engpress/pages/search.aspx?i=003-3714372-4232718#{"itemid":["003-3714372-4232718"]}

48 Either under national law or by decision of the supervisory authority.

Whether the processing of sensitive data is justified by reasons of substantial public interest must be reviewed on a case-by-case basis. However, the criteria for such assessment can be deduced from Article 8(2) ECHR and the related jurisprudence from the ECrtHR:[49]

- The processing of sensitive data must serve a legitimate aim;
- The means (i. e. the processing of sensitive data) must be proportional to the aim (principle of proportionality);
- There must be no other less severe means to achieve the aim (principle of subsidiarity).

This means that also when a substantial public interest exists, it must be determined if the processing of sensitive data is also necessary in light of this interest ('necessity test'). That is: the means (i. e. the processing of sensitive data) must be suitable to achieve the aim, it must be proportional to the aim and there should be no less severe means available with which the aim could also be achieved. Also the Working Party identified a need to clarify the condition "for reasons of substantial public interest"[50]. It recommends taking Art. 52 (1) of the EU Charter of Fundamental Rights as a model and to allow for the processing of sensitive personal data only if provided for by a legal act which clearly sets out the aims and grounds, including the substantial public interest at stake, for the processing of such data.

In addition to the condition of a substantial public interest, suitable safeguards should be provided. The suitability of these safeguards is dependent on the circumstances of the case at hand. The question whether a safeguard is in fact 'suitable' will be variable over time, for example, in relation to technological developments regarding data security. The ECrtHR sets a higher standard of (legal) safeguards for the protection of privacy in relation to processing sensitive data.[51] These include, among others, guarantees that

49 See e. g. ECrtHR, 4 December 2008, Application No 30562/04 and 30566/04, S. and Marper v. United Kingdom; ECrtHR, 18 May 2010, Application No 26839/05, Kennedy v. United Kingdom.

50 Article 29 Working Party "Advice paper on special categories of data (sensitive data)", p. 11.

51 See e. g. ECrtHR, 4 December 2008, Application No. 30562/04 and 30566/04, S. and Marper v. United Kingdom; and ECrtHR, 20 January 2010, Application No. 20689/08, W. v The Netherlands.

no more data than strictly necessary are registered, limitations in regard to the retention period of the data, and duty to confidentiality provisions. Moreover, it should be laid down by law who is responsible for the processing of the data and who has access to the data.

Conclusion

It can be concluded that at least data on trafficked persons' involvement in prostitution should be qualified as "sensitive data". This implies that strict conditions on the processing of such data must be met in order to justify an exception on the general prohibition on the processing of sensitive data. It is questionable if in practice these conditions are met in all cases where data on trafficked persons are collected, retained, and exchanged.

When it comes to persons trafficked for purposes other than the sex industry, it is less clear whether personal data gathered in these cases also should be qualified as 'sensitive data' and thus be dealt with under a stricter regime. This needs more research.

However, no matter in which industry trafficked persons were exploited, the collection and processing of data regarding their health and ethnic background could be similarly argued to constitute 'sensitive data' with the consequences entailed.

Summary

The Data Protection Directive provides for a set of rights for individuals, such as the right to access, rectify, block and delete their own data, as well as the right to receive information for what purposes and by whom their data are processed. It also provides judicial remedies as well as the right to receive compensation for damage suffered. These rights are, however, expressed in general terms and it is not clearly specified how they can actually be exercised.

Moreover, as noted by the European Commission in its 2012 Impact Assessment[52], fragmentation and inconsistent implementation and enforcement mean that rights vary among the different Member States, and often individuals are neither aware nor in control of what happens to their personal data and as a result fail to exercise their rights effectively. Such issues have led to proposals for a new EU framework for data protection. In regard to the protection of data of trafficked persons, it should be noted that the Directive applies to both the public and private sector, including international and intergovernmental organisations, NGOs, and (commercial) businesses.

Of particular interest is the potential for greater protections for persons trafficked for prostitution. It may be argued that data on persons trafficked for prostitution should be classified as 'sensitive data', and thus subject to a stricter regime. This has consequences for the collection, retention and exchange of data on trafficked persons[53] without their informed and freely given consent, for example, in the framework of international referrals.

Council of Europe Data Protection Convention (Convention 108)

Overview of relevant provisions

The Convention for the Protection of Individuals with regard to automatic processing of personal data, also known as Convention 108, was adopted by the Council of Europe in 1981. It was the first legally binding international instrument adopted in the field of data protection designed:

> » [T]o secure [...] for every individual [...] respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data. (art.1)

52 European Commission Impact Assessment SEC(2012)72 final, Annex 2, p. 21; http://ec.europa.eu/justice/data-protection/document/review2012/sec_2012_72_en.pdf.

53 Other than in the context of police and judicial cooperation in criminal matters.

Convention 108 sets out minimum standards aimed at protecting individuals against abuse of their personal data, and it regulates the transborder flow of personal data. According to article 11, parties to the Convention may set higher standards at the national level.[54] Currently the Convention has been ratified by forty-four Member States of the Council of Europe, including all EU Member States.[55] As the Convention is also open to non-Member States, other third countries are likely to ratify in the future. In 2012 the Council of Europe and the Convention's Consultative Committee began a process to update this legal instrument with two main objectives:

- to address privacy challenges resulting from the use of new internet and communication technologies (ICTs); and
- to strengthen the Convention's follow-up mechanism.

Scope of application

Although Convention 108 is the precursor of the Data Protection Directive and may be assumed to have a similar focus and scope of application, there are some major differences.

To date, the Convention still remains the only binding international legal instrument in the field of data protection with a *worldwide* scope of application, open to any country, including countries which are not Members of the Council of Europe. The Convention protects against privacy intrusions by public and private authorities whether offline or online. Contrary to the Data Protection Directive, it also covers activities in the areas of defence, national security or law enforcement. It is important to note that the definition of automatic processing in Convention 108 does not include the *collection* of data. The only provision applying to the collection of personal data is Article 5(e)

54 According to paragraph 48 of the Explanatory Report to Convention 108, the contracting parties to the Convention may set higher standards of protection for additional categories of data "depending on the legal and sociological context in the country concerned"; http://conventions.coe.int/Treaty/en/Reports/Html/108.htm.

55 Status as of 8 March 2013. For an overview of the Member States: http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=108&CL=ENG.

which states that personal data undergoing automatic processing should be "obtained and processed fairly and lawfully", be "adequate, relevant and not excessive", and "accurate".

Principles and conditions for processing data

The main provision on data quality is article 5, which is comparable to article 6 of the Data Protection Directive, but has a more limited scope.

Article 5 Convention 108 – Quality of data

Personal data undergoing automatic processing shall be:

a) obtained and processed fairly and lawfully;

b) stored for specified and legitimate purposes and not used in a way incompatible with those purposes;

c) adequate, relevant and not excessive in relation to the purposes for which they are stored;

d) accurate and, where necessary, kept up to date;

e) preserved in a form which permits identification of the data subjects for no longer than required for the purpose for which those data are stored.

However, article 9(2) of the CoE Convention, allows for wide-ranging exceptions, including the possibility for Member States to derogate from the provisions regarding quality of data (art. 5), sensitive data (art. 6) and additional safeguards for data subjects (art. 8):

» [W]hen such derogation is provided for by the law of the Party and constitutes a necessary measure in a democratic society in the interests of:

a) protecting State security, public safety, the monetary interests of the State or the suppression of criminal offences,

b) protecting the data subject or the rights and freedoms of others.

Sensitive data

Similar to the Directive, Convention 108 contains specific provisions on the processing of sensitive data. Article 6 on special categories of data states:

> » Personal data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life, may not be processed automatically unless domestic law provides appropriate safeguards. The same shall apply to personal data relating to criminal convictions.

With the exception of the categories ethnic origin, philosophical beliefs, trade-union membership and personal data relating to criminal convictions, the Convention covers the same type of sensitive data as Article 8 of the Data Protection Directive. The Convention does not further define the various categories of special data nor what constitutes "appropriate safeguards", thus leaving the parties significant discretion. The exceptions of article 9(2) also apply to sensitive data.

Sanctions

The Convention requires Member States to embody its principles in domestic law and establish appropriate sanctions and remedies for violations of these principles (art. 10). Such sanctions and remedies can be of differing nature (civil, administrative or criminal), depending on the specific situation in each of the States. There is no requirement for additional mechanisms such as a supervisory authority, nor does it oblige contracting parties to establish institutional mechanisms for the independent investigation of complaints. To remedy these weaknesses an additional protocol entered into force on 1 July 2004 which requires parties to set up a supervisory authority, exercising its functions in complete independence, as an essential element of the effective protection of individuals.[56]

56 Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows (CETS No.: 181).

3. THE CONCEPT OF 'SENSITIVE DATA' AND MANDATORY REGISTRATION OF SEX WORKERS AS AN ANTI-TRAFFICKING MEASURE: THE CASE OF THE NETHERLANDS[57]

This chapter will look into a concrete example of the application of 'sensitive data' by discussing the case of mandatory registration of sex workers in the Netherlands. In 2009 a new Bill on prostitution was submitted to the Dutch Parliament, partly justified by the wish to combat trafficking. As part of a wider range of measures, the Bill introduced mandatory registration of sex workers and the criminalisation of unregistered sex workers and their clients.

While the formal aim of the Bill was to facilitate control and enforcement in the sex sector, it was argued that mandatory registration would help to combat trafficking by providing insight into who were working as prostitutes and where they were working. In addition, according to the minister, registration would provide for a 'contact moment' with sex workers so that victims might be identified and sex workers could be informed about their rights and the possibilities to access support services.

The Bill met with massive resistance from sex workers, service providers, experts, academics, and others working in the field of sex work and trafficking. Apart from the fact that almost no one believed that mandatory registration would help to combat trafficking, it was also obvious that a national register of sex workers would be extremely privacy sensitive.

This raised the question as to whether mandatory registration of sex workers would fall under the prohibition on the processing of data concerning someone's sex life (article 8 Data Protection Directive; article 16 Dutch Personal Data Protection Act[58]).

57 This chapter is based on the legal research carried out by Van der Feltz advocaten (W. I. Koelewijn & R. L. de Graaff), commissioned by the Dutch Association of Women and Law (VVR), on the compatibility of the 2009 Bill on mandatory registration of sex workers with the Data Protection Directive and its corresponding provisions in Dutch law.

58 Wet bescherming persoonsgegevens (Wbp). The Wbp is the transposition of the Data Protection Directive; its provisions should therefore be interpreted in conformity with the Directive.

According to the advice of the Council of State[59] this was the case. This would imply that in order to justify mandatory registration it should be necessary for reasons of substantial public interest, suitable safeguards should be provided to protect private life and it should have a legal basis. In the opinion of the Council of State the aim of facilitating control and enforcement was not in proportion to the proposed means, that is a general obligation for sex workers to register. Consequently, the Council of State held that the Bill would not stand the 'necessity test', nor was there a 'substantial public interest'.

The Dutch Minister of the Interior, however, set aside the critique of the Council of State arguing that sex work should be regarded as work and that therefore the prohibition of article 16 of the Dutch Data Protection Act (the transposition of article 8 Directive) was not applicable. According to his opinion data on the fact that a person worked in prostitution could not be considered as data on someone's 'sex life', as it referred to the person's professional (sex) life and not to his or her private sex life, sexual preferences or sexual orientation.

It thus became important to investigate how the concept of 'sex life' was interpreted in EU law and whether there was justification for making a distinction between a person's private and professional sex life.

As previously noted 'sex life' is neither defined nor explained in the Directive or its preamble. Nor does the jurisprudence of the EU Court of Justice (ECJ) provide for the interpretation of the concept of 'sex life'. However, the ECrtHR has judged in several cases that sexuality is part of the most intimate aspects of someone's privacy, which means that in a democratic society only especially serious reasons can justify interference of the government.[60]

Moreover, both the case law of the ECJ and the ECrtHR do not support the distinction between a person's professional and private life. In this regard

59 Raad van State, No.W04.09.01 50/1, 11 September 2009. The Council of State is an advisory body to the government.

60 ECrtHR, 22 October 1981, Appl. No. 7525/76, Dudgeon v. UK; ECrtHR, 26 October 1988, Appl. No. 10581/83, Norris v. Ireland.

the ECJ refers to the ECrtHR, which held in several cases that "the term 'private life' should not be interpreted restrictively" and that "there is no reason of principle to justify excluding activities of a professional or business nature from the notion of 'private life'"[61]. This especially applies in the case of a person exercising a liberal profession where "professional and non-professional activities [are] so intermingled that there [is] no means of distinguishing between them"[62]. This was confirmed in the previously discussed case of *Khelili v. Switzerland*.[63]

In addition, at the time of the adoption of the Dutch Personal Data Protection Act in 1999, the then Minister of Justice had answered on the question as to whether the notion of 'sex life' also covered, for example, promiscuity:

» Promiscuity, or the question if people go on a regular basis to the Red Light District, falls under sex life. This is therefore not the same as sexual orientation.[64]

It was difficult to maintain that visiting a sex worker would qualify as sensitive data while working as a sex worker would not. Furthermore, it followed from Dutch case law that it is the nature of the data rather than the aim for which the data is processed that is decisive in determining whether the data is 'sensitive'.[65]

It could therefore be concluded that the distinction between one's professional and personal sex life, made by the Minister, would not stand the test of both the ECJ and the ECrtHR. This forced the Minister of Justice to admit that the distinction between the professional and private life of sex workers could not be maintained, and that, contrary to his previous statement,

61 EU Court of Justice, C-92/09 and C93/09 of 9 November 2010, Schecke & Eifert, § 59; see also EU Court of Justice, C-456/00, Österreichischer Rundfunk and Others, §§ 73 and 74; EU Court of Justice, 8 November 2007, T-194/04, Bavarian Lager Co. Ltd; and ECrtHR 16 December 1992, Application No. 13710/88, Niemietz v. Germany, § 29.

62 ECrtHR 16 December 1992, Application No. 13710/88, Niemietz v. Germany, § 29.

63 ECrtHR of 18 October 2011, Application No. 16188/07, Khelili v. Switzerland, § 56.

64 Kamerstukken II 1998–1999, 14 781, nr. 8, p. 23.

65 Hoge Raad, 23 March 2010, LJN BK6331.

registration of sex workers indeed concerned the processing of sensitive data and thus fell under the general prohibition of article 16 of the Dutch Personal Data Protection Act.

The next question was whether the conditions for an exception to this prohibition could be satisfied. According to article 23 (1) sub f of the Dutch Personal Data Protection Act (article 8 Directive), an exception on the general prohibition to process sensitive data is only justified under strict conditions. In line with the Directive it must be necessary for reasons of substantial public interest, subject to the provision of suitable safeguards and have a legal basis.[66]

Following Dutch case law, the question as to whether or not there is a legitimate aim justifying processing sensitive data, must be judged in light of the nature, seriousness and extent of the problem that it aims to solve.[67] If there is indeed a substantial public interest, then a further determination must be made as to whether the processing of sensitive data is also *necessary* in light of this interest. In the context of this 'necessity test' it follows from European jurisprudence – as discussed in the previous chapter – that the means (i.e. the processing of sensitive data) must be suitable to achieve the aim, that they must be proportional to the aim and that there should be no less severe means available with which the aim could also be achieved.

To assess whether an exception could be legitimised by "reasons of substantial public interest", one had to look at the aims of the Bill. Despite the rhetoric about combating trafficking, the aim of the Bill, in the end, boiled down to "to regulate prostitution and sex businesses" and "to facilitate control and enforcement". It was highly doubtful whether this aim justified a serious violation of the privacy of all sex workers in the Netherlands. This led to the question whether registration was proportional to the aim. Significantly, the Bill lacked motivation in regard to the nature, seriousness and extent of abuses in the sex sector, which would constitute such a serious public interest that it would justify the violation of sex workers' right to

66 Either by national law or by decision of the supervisory authority.

67 See e.g. ABRvS 3 September 2008, LJN BE9698.

privacy. In addition, there were other, more effective means available to achieve the aims of the Bill which would constitute a less invasive violation of the privacy of sex workers. For example, intensifying monitoring of sex businesses rather than individual workers and expanding outreach services to sex workers in order to establish contacts and provide them with information and assistance.

An important factor underlining the doubts about the effectivity, suitability and proportionality of mandatory registration was the fact that a large number of NGOs, sex workers, service providers, jurists and other professionals expressed their concerns about potential adverse effects, such as sex workers shifting into the unregulated, illegal sex sector and disappearing out of sight of health and other service providers. This concern was reflected in the 2010 Concluding Observations of the CEDAW Committee:[68]

» 30. The Committee is concerned that the new bill on prostitution in the Netherlands making the registration of prostitutes compulsory may lead the majority of prostitutes to work illegally. Among those prostitutes are migrant women from third countries who will not have the possibility of registering. The Committee is therefore concerned that the law, rather than improving the situation of prostitutes, might on the contrary undermine efforts to combat the sexual exploitation of women and increase the vulnerability of prostitutes who are not able or not willing to register by worsening their working conditions and exacerbating their social exclusion. The Committee expresses concern that this new legislation may also create serious risks for registered prostitutes' privacy and safety.

31. The Committee urges the State Party to carefully conduct a risk assessment of the new law, including from the perspective of privacy, in consultation with concerned groups and relevant organizations before adopting it. The Committee also

68 Concluding Observations of the Committee on the Elimination of Discrimination against Women, The Netherlands, CEDAW/C/NLD/CO/5, 5 February 2010, p. 7–8. The concerns expressed by the Committee followed the concerns in the shadow report submitted by the Dutch NGOs.

> calls upon the Netherlands to provide more comprehensive and concrete information in its next periodic report on the measures taken to improve the working conditions of prostitutes and to enhance their autonomy, privacy and safety.

Other arguments were the lack of suitable safeguards for the protection of the privacy of sex workers, keeping in mind the high level of standards the ECrtHR sets in the case of sensitive data.[69]

Finally, if the registration data would also be accessible for police, its processing would be subject to the regime of the Police Act. Since other rules apply to police data in regard to retention duration and processing possibilities, registration raised the risk that data on sex workers would be retained in police databases despite duration provisions in the Data Protection Act and the Bill for the removal of personal data from the central database. Moreover, the Police Act allows for the exchange of data with other police forces and third parties, including foreign police forces. The latter might put migrant sex workers at risk when returning to their home country, especially in cases where their national law criminalised sex workers.

In July 2013, following serious objections of the first Chamber of Parliament (Senate) against the mandatory registration of sex workers, the Minister was forced to withdraw the Bill.

69 See e. g. ECrtHR, 4 December 2008, Application No. 30562/04 and 30566/04, S. and Marper v. United Kingdom; and ECrtHR, 20 January 2010, Application No. 20689/08, W. v The Netherlands.

4. SPECIFIC DATA PROTECTION PROVISIONS IN ANTI-TRAFFICKING LEGAL INSTRUMENTS

This chapter explores existing data protection and privacy rights provisions in current European anti-trafficking law, policy tools and other 'soft law' recommendations.

a. Council of Europe Convention on Action against Trafficking in Human Beings

The Council of Europe Convention on Action against Trafficking in Human Beings (hereafter "CoE Trafficking Convention") states that all personal data regarding trafficked persons shall be used in conformity with Convention 108[70], regardless of whether Member States have ratified.[71]

The provision on protection of private life is contained in Article 11 of the CoE Trafficking Convention:

» 1. Each Party shall protect the private life and identity of victims. Personal data regarding them shall be stored and used in conformity with the conditions provided for by the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 108).
2. Each Party shall adopt measures to ensure, in particular, that the identity, or details allowing the identification, of a child victim of trafficking are not made publicly known, through the media or by any other means, except, in exceptional circumstances, in order to facilitate the tracing of family members or otherwise secure the well-being and protection of the child.

70 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, also known as "Convention 108". This convention was the first legally binding instrument in the data protection field and entered into force on 1 October 1985. It has been ratified by 44 Member States of the Council of Europe, including all EU Member States.

71 CoE Convention on Action against Trafficking in Human Beings Explanatory Report, article 11:141; http://www.conventions.coe.int/Treaty/EN/Reports/Html/197.htm.

3. Each Party shall consider adopting, in accordance with Article 10 of the Convention for the Protection of Human Rights and Fundamental Freedoms as interpreted by the European Court of Human Rights, measures aimed at encouraging the media to protect the private life and identity of victims through self-regulation or through regulatory or co-regulatory measures.

As stated in the Explanatory Report of the CoE Trafficking Convention, the protection of trafficking victims' private life and identity is essential for their physical safety, given the danger from their traffickers, as well as (on account of the feelings of shame and the risk of stigmatization, both for the victim and the family), to preserve their chances of social reintegration in the country of origin or destination or into receiving countries.[72] Private life is also dealt with in Article 30 of the Convention[73], which is concerned with protection of victims' private life and identity in the specific context of judicial proceedings.

With regard to children, Article 11(2) provides for special protection measures to ensure that the identity or details allowing for the identification of a child victim of trafficking are not made public. Under exceptional circumstances, releasing information about a child victim's identity may be justified in order to trace relatives or otherwise secure the wellbeing and protection of the child. The Parties, however, are free to decide what measures they take to prevent this. Some countries impose criminal penalties for publicly revealing any information that might lead to the identification of victims of some offences.[74]

72 CoE Convention on Action against Trafficking in Human Beings Explanatory Report, article 11:138.

73 Article 30 – Court proceedings: In accordance with the Convention for the Protection of Human Rights and Fundamental Freedoms, in particular Article 6, each Party shall adopt such legislative or other measures as may be necessary to ensure in the course of judicial proceedings: a. the protection of victims' private life and, where appropriate, identity; b. victims' safety and protection from intimidation, in accordance with the conditions under its internal law and, in the case of child victims, by taking special care of children's needs and ensuring their right to special protection measures.

74 CoE Convention on Action against Trafficking in Human Beings Explanatory Report, article 11:143.

Finally, article 11(3) prescribes Parties to adopt measures encouraging the media to protect victims' private life and identity. To avoid undue interference with media freedom of expression, it states that such measures must accord with article 10 ECHR and must be for the specific purpose of protecting victims' private life and identity.

b. UN Protocol to Prevent, Suppress and Punish Trafficking in Persons, especially Women and Children

The Protocol to Prevent, Suppress and Punish Trafficking in Persons, especially Women and Children, supplementing the United Nations Convention against Transnational Organized Crime (UN Trafficking Protocol), is the first global legally binding instrument with an agreed definition on trafficking in persons. The UN Trafficking Protocol does not contain any provisions on data protection or processing. Article 10 states only that "law enforcement, immigration or other relevant authorities of State Parties shall, as appropriate, cooperate with one another by exchanging information, in accordance with their domestic law [...]".

c. Directive 2011/36/EU of 5 April 2011 on preventing and combating trafficking in human beings and protecting its victims

Directive 2011/36/EU of 5 April 2011 on preventing and combating trafficking in human beings and protecting its victims (Trafficking Directive), provides binding legislation to prevent trafficking, to effectively prosecute criminals, and to better protect the victims. Recital 33 of the Directive confirms its respect for fundamental rights and its observance of the principles:

> » [R]ecognised in particular by the Charter of Fundamental Rights of the European Union and notably [...] the protection of personal data [...]." In particular, the Directive "seeks to ensure full respect for those rights and principles and must be implemented accordingly.

5. DATA PROTECTION CHALLENGES IN ANTI-TRAFFICKING POLICIES

The chapter discusses the applications of data protection law and anti-trafficking interventions for the purpose of practical adoption. In addition, it suggests recommendations for anti-trafficking stakeholders, with the main focus on anti-trafficking NGOs.

Overview

National Rapporteur and other data collection tools	
Challenges	• Data collection of trafficked persons may include personal data
datACT recommendations	• Setting standards for NGO cooperation • Advocacy to use only anonymous data
Identification of trafficked persons and access to support structures	
Challenges	• Registration and transfer of victims' personal data between countries of origin and destination, and between national agencies
datACT recommendations	• Conducting Privacy Impact Assessment (PIA) • Avoiding the transfer of personal data to the possible extent • Maintaining and advocating for a decentralised and anonymous access services for trafficked persons
NGO service providers	
Challenges	• Internal ICT case documentation and management system may not be secure • NGO counsellors may be forced to share personal data of victims with law enforcement and prosecution personnel • Victims' rights as data subject may not be an integral part of the counselling process
datACT recommendations	• Establishing secure ICT soft- and hardware in NGO counselling centres based on a PIA • Advocating for stronger protection of the obligation to confidentiality and the right to refuse to give evidence in court • Introducing counselling modules on the right to privacy

5.1 National Rapporteur and other data collection tools

Challenge: Data collection of trafficked persons may include personal data

datACT recommendations:

- Setting standards for NGO cooperation with National Rapporteur or Equivalent Mechanism
- Advocacy to share only anonymous data

During recent years, several data collection procedures were developed at the national and global level in order to gain better understanding about the trends and extent of human trafficking. The idea of a systematic and coordinated collection mechanism of data on trafficking in human beings was developed within the framework of 'The EU Hague Ministerial Declaration 1997':

> Provide or explore the possibilities for the appointment of national rapporteurs, who report to Governments on the scale, the prevention and combating of trafficking in women. Develop criteria for reporting on the scale, nature and mechanisms of trafficking in women and the effectiveness of policies and measures concerning these phenomena. Encourage the cooperation of national rapporteurs on a regular basis. (Art. III.1.4)[75]

While this remained an optional tool for more than a decade in most legal and political anti-trafficking instruments in Europe, including the OSCE, the EU and the CoE, in 2011 the establishment of a National Rapporteur or Equivalent Mechanism became mandatory for EU Member States. Article 19 of the Directive 2011/36 EU binds Member States to take all necessary steps in order to establish National Rapporteur Mechanisms or

75 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.legislationline.org.

equivalent structures.[76] Governments should seek cooperation with civil society organisations for gathering all necessary data.

> Member States shall take the necessary measures to establish national rapporteurs or equivalent mechanisms. The tasks of such mechanisms shall include the carrying out of assessments of trends in trafficking in human beings, the measuring of results of anti-trafficking actions, including the gathering of statistics in close cooperation with relevant civil society organisations active in this field, and reporting. (Art. 19)[77]

In its comment on the Directive, the UN joint agencies state that data collection should cover harmonised sex and age disaggregated data, based on common definitions and a common understanding of key concepts, and cover all forms of trafficking:

> [W]hile fully respecting the protection of the privacy of trafficked persons and in accordance with the Directive on the Protection of individuals with regard to the processing of personal data and on the free movement of such data.[78]

Political recommendations on data collection systems in Europe

Over the past decade there have been numerous recommendations, guidelines, and legal provisions calling for National Rapporteur structures or equivalent mechanisms. The 2005 Council of Europe Convention on Action against Trafficking in Human Beings encourages state parties to:

76 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.

77 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.

78 Prevent. Combat. Protect. Human Trafficking. Joint UN Commentary on the EU Directive – A Human Rights-Based Approach, November 2011, p. 100; http://www.unhcr.org/4ee6215e9.html.

» [C]onsider appointing National Rapporteurs or other mechanisms for monitoring the anti-trafficking activities of State institutions and the implementation of national legislation requirements. (Art 29(4))

It also requires from the state parties to protect the private life of victims (Art.11(1)3). In 2006 the OSCE Ministerial Council published Decision No.14, "Enhancing efforts to combat trafficking in human beings, including for labour exploitation, through a comprehensive and proactive approach", urging participating States:

» [W]ith the support of the OSCE structures and institutions if requested, to improve research and the system of data collection and analysis, with regard to the confidentiality of data, and where possible to disaggregate statistics by sex, age, and other relevant factors as appropriate, in order to better assess the character and scope of the problem and develop effective and well-targeted policies on trafficking in human beings. To this end, participating States are recommended to consider appointing National Rapporteurs or similar independent monitoring mechanisms. (Art. 3)[79]

In 2008 the Alliance against Trafficking in Persons, an informal network of international organisations and NGOs[80], issued a statement on the definition of a National Rapporteur or Equivalent Mechanism (NREM). It describes the role of a National Rapporteur in a more detailed manner:

» In general, the recommendations made to such a mechanism aimed at:
1. Identification of the scale of the problem
2. encouraging the exchange of information among counterparts at international level

79 OSCE Decision No.14/06 Enhancing Efforts to Combat Trafficking in Human Beings, including for Labour Exploitation, through a Comprehensive and Proactive Approach. MC.DEC/14/06.

80 The Alliance against Trafficking in Persons gathers regularly under the auspices of the OSCE.

3. calling upon the mechanism to draw up annual reports for government discussion at national level with a view to developing appropriate policies (e. g. Parliamentary debate); and
4. encouraging research in order to better understand and address this phenomenon.

[...] One can confirm the advantages of such a function by having better conceptualization of trends, efforts and responses at State level in relation to THB, including the significant impact on national policies and legislation.[81]

Similar soft-law recommendations on data collection and the role of National Rapporteurs were developed within the context of the European Union. In 2009, the EU Council issued a document with conclusions recommending 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:

» 4. The network should complement agreed activities based on the existing EU instruments and carried out by existing EU structures. In particular, the network should not interfere with law enforcement and judicial co-operation, e. g. by exchanging findings of investigations, including personal data.
5. Each Member State, on the basis of national conditions, is invited to designate a National Rapporteur or equivalent mechanism, with the scope of activity that includes collection of information and advising on human trafficking to participate in the activities of the network.[82]

81 Presented by the OSCE Special Representative for Combating Trafficking in Human Beings (SR), on behalf of the Alliance Expert Coordination Team (AECT), 16 October 2008.

82 Council of the European Union, council conclusions 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. Presented by the OSCE Special Representative for Combating Trafficking in Human Beings (SR), on behalf of the Alliance Expert Coordination Team (AECT), 16 October 2008.

On 19 June 2012, the European Commission adopted the "**EU Strategy towards the Eradication of Trafficking in Human Beings (2012–2016)"**[83]. The Strategy is a set of concrete and practical measures to be implemented within a five-year timeframe. It is based on five key priorities:

a. Identifying, protecting and assisting victims of trafficking;
b. Stepping up the prevention of trafficking in human beings;
c. Increased prosecution of traffickers;
d. Enhanced coordination and cooperation among key actors and policy coherence;
e. Increased knowledge of and effective response to emerging concerns related to all forms of trafficking in human beings.

As for data collection tools, the EU Strategy refers to the legally binding EU Directive 2011/36/EU on Preventing and Combating Trafficking in Human Beings and Protecting its Victims. Member States are obliged to implement the Directive within a clearly defined timeframe.

The EU Strategy suggests the following procedure:

Data collection systems
Action 1 under Priority E 'Increased knowledge of and effective response to emerging concerns related to all forms of trafficking in human beings' dictates the development of an EU-wide system for data collection with the aim of collecting reliable, comparable data for evidence-based policy on trafficking in human beings and understanding the flows and trends of internal trafficking.[84]

The European Data Protection Supervisor (EDPS) reviewed the EU Strategies and issued comments regarding:

83 COM(2012)286 final – The EU Strategy towards the Eradication of Trafficking in Human Bengs 2012–2016, 19 June 2012; http://ec.europa.eu/dgs/home-affairs/e-library/docs/thb_strategy/thb_strategy_en.pdf.

84 EU Strategy, p. 13.

- Data protection as a pre-condition to mutual trust between the victims and the authorities involved in prevention, protection and prosecution;
- Data protection as part of the victims' rights, in particular the right to information;
- Data protection in the development of an EU-wide System for Data Collection;
- Data protection as a strategy to assist Member States in addressing fundamental rights issues specifically related to anti-trafficking policy and related actions.[85]

This document is one of the few EU documents that considers data protection a necessary element in its recommendations on data collection. The EDPS recommended that in its implementation phase the EU Strategy would strongly benefit from the inclusion of a data protection perspective and further clarification on how data protection can help this area. In addition, in its recommendations the EDPS stressed that the information given to victims of trafficking should include both information on the right to the protection of personal data and on the procedures to be followed in order to effectively exercise this right.

Existing European and global data collection tools and reports

During recent years, several data collection procedures have been developed on a global and European level. While they all aim at quantifying trafficking in human beings, they approach the issue from different methodological and conceptual angles. Some of the global data collection tools generate their own data based on their direct involvement in anti-trafficking work (IOM), others seek to systematically assess existing data provided by National Rapporteur or Similar Mechanisms (US State Department, UNODC, Eurostat). Other approaches involve providing elaborated guidelines to national governments for data collection (ICMPD), or initiatives developing estimated data on human trafficking and forced labour (ILO).

85 EDPS Comments on the EU Strategy, see footnote 14.

Examples of data collection systems

Since 2001, the US State Department collects general data on trafficking, including an evaluation on policy responses in the areas of prevention, protection, and prosecution. It publishes the global Report on Trafficking in Persons (TIP report) annually. Since 2005 the report also includes global data on numbers of identified trafficked persons, prosecutions, and convictions.

The International Centre for Migration Policy Development (ICMPD) developed guidelines for European governments on collecting data on human trafficking. Even though the recommendations refer to national and European data protection legislation the guidelines still suggest collecting personal data of victims.[86] The International Organisation for Migration (IOM), a leading international organisation in anti-trafficking policies, even operates a global data base on human trafficking:

» For more than a decade, IOM has developed and maintained a standardized counter-trafficking data management tool, the Counter-Trafficking Module (CTM), which is the largest global database with primary data on victims of trafficking.

The CTM facilitates the management of all IOM direct assistance, movement and reintegration processes through a centrally managed system, as well as mapping victims' trafficking experiences. In return, the database strengthens research capacity and the understanding of the causes, processes, trends and consequences of trafficking. It serves as a knowledge bank from which statistics and detailed reports can be drawn, and information be provided for research, programme development and policy-making on counter-trafficking.

In all cases, IOM ensures that no information which could compromise the privacy or identity of trafficked individuals is

86 International Centre for Policy Development; http://www.icmpd.org/fileadmin/ICMPD-Website/ICMPD-Website_2011/Capacity_building/THB/Publications/DCIM-EU_Handbook.en.pdf.

released: strict controls designed to ensure confidentiality and security of all data have been established.[87]

In 2012 The International Labour Organisation (ILO) published a second global estimation of people who are forced into labour.[88] At that time the ILO assessed that worldwide 20.9 Million people were forced labourers.[89] However, this estimation is not based on information gathered from a global data base with primary data on human beings identified as forced labourers by ILO. Instead, the methodology that lead to the ILO figures derive from a compilation of reported cases drawn from various sources:

» The method relies on the collection of "reported cases" of forced labour, over the 10 year period 2002–2011, from all countries in the world. "Reported cases" are those which refer to specific instances of forced labour, indicating where and when the activity took place and how many people were involved. Cases can be found in various secondary sources of information, ranging from official statistics and NGO reports to newspaper articles.[90]

In 2010 the UNODC was mandated by the UN General Assembly to conduct global reports on trends and patterns of human trafficking.[91] In 2012 the UNODC published its first global report on trafficking in hu-

87 Quotation from: http://www.iom.int/cms/countertrafficking.

88 The first ILO report on forced labour was published in 2005: International Labor Organisation: A global alliance against forced labour. Global report under the follow-up to the ILO Declaration on Fundamental Principles and Rights at Work. Report of the Director-General, 2005.

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

90 See ILO 2012 Global Estimate of Forced Labour – Executive Summary, p. 5; http://www.ilo.org/wcmsp5/groups/public/–ed_norm/–declaration/documents/publication/wcms_181953.pdf

91 In paragraph 60 of the Plan of Action, UNODC is assigned the mandate and duty to collect relevant data and report on trafficking in persons patterns and flows at the national, regional and international levels: Request the Secretary-General, as a matter of priority, to strengthen the capacity of the United Nations Office on Drugs and Crime to collect information and report biennially, starting in 2012, on patterns and flows of trafficking in persons at the national, regional and international levels in a balanced, reliable and comprehensive manner, in close cooperation and collaboration with Member States, and share best practices and lessons learned from various initiatives and mechanisms. (Assembly resolution 64/293, para. 60). See www.unodc.org/unodc/en/human-trafficking-fund/hum.

man beings.[92] Similar to the 2012 EU Strategy, the UNODC report uses percentages to describe the global quantity of victims and perpetrators of trafficking, and refrains from presenting absolute figures. As with the ILO 2012 report the methodology for the UNODC report relies on secondary sources, such as national government crime statistics, NGO annual reports etc.:

» The vast majority of the data collected for this *Global Report on Trafficking in Persons* came from national institutions (88 per cent of the data series collected). Other sources of information were international governmental organizations (5 per cent of the data) and non-governmental organizations (7 per cent).The information was collected by UNODC in three ways: through a short, dedicated questionnaire distributed to Governments; by considering the relevant results of the regular United Nations Survey of Crime Trends and Operations of Criminal Justice Systems used to survey Member States on official statistics on different forms of crime; and by collecting official information available in the public domain (national police reports, Ministry of Justice reports, national trafficking in persons reports etc.).

In 2013, The European Commission, in cooperation with Eurostat, issued statistics on trafficking cases in its Member States for the first time and provided figures from the year 2008 to 2010. These figures are conceptualised into 'identified' and 'presumed' victim categories. The concepts of 'identified' and 'presumed' victim is not clearly defined and raise concerns about the consistency across the gathered statistics.

As for 2010, the report documents 9582 identified and presumed trafficked persons in EU Member States.[93] The Eurostat report also relies on secondary data from existing statistics in the Member States:

92 See http://www.unodc.org/documents/data-and-analysis/glotip/Trafficking_in_Persons_2012_web.pdf.

93 See http://ec.europa.eu/dgs/home-affairs/what-is-new/news/news/2013/docs/20130415_thb_stats_report_en.pdf, p. 14.

» Consistent with the integrated approach in addressing trafficking in human beings, data were requested from different services and organisations working in the field of trafficking in human beings in the participating countries, such as the police, prosecution services, court services, immigration services, border guards, labour inspectors as well as non-governmental organisations.

The questionnaire was sent via Eurostat to the National Statistical Offices of the EU Member States, EU Candidate and Potential Candidate countries and to the EFTA/EEA (European Free Trade Association/European Economic Association) countries in September 2011. It included the appropriate tables, a list of common indicators, definitions and guidelines for collecting the statistical data as well as the country codes to be used and a template for providing metadata. The data received from participating countries were then included in tables and returned to the countries for validation in August 2012. The tables were finalised by Eurostat in December 2012.[94]

Additional selected data collection bases, guidelines and tools:

- IOM Global Human Trafficking Data Base Counter Trafficking Division (CTM)
- ICMPD Data Collection and Information Management (DCIM) and Data collection guidelines
- ILO and EC: Delphi survey
- UNODC – UN.GIFT Global Report on TIP depict patterns and trafficking flows for 155 countries and territories
- IOM and the Austrian Ministry of Interior: Development of Guidelines for the Collection of Data on Trafficking in Human Beings, including comparable indicators/variables 2008
- Montrasec demo (University Ghent)
- Europol Information System (EIS) and Analysis Work Files (AWF Phoenix 2007)

94 See http://ec.europa.eu/dgs/home-affairs/what-is-new/news/news/2013/docs/20130415_thb_stats_report_en.pdf, p. 21.

datACT recommendations

In summary, the legal provisions remain vague on the definition for data collection tools such as National Rapporteur or similar Mechanisms (NREM). Moreover, the role of NGOs in cooperating with data collection tools is also not clear. The diversity of existing data collection tools hinders the elaboration for clear guidelines governing the actions of stakeholders. Applying data protection provisions on data collection tools, datACT recommends following principles:

- The protection of the trafficked persons' privacy should be at the core of all data collection measures.
- All data collection efforts should follow recognised ethical data protection methods, such as 'Privacy by Design'[95] and 'Privacy Impact Assessments'[96].
- NGO counselling centres should not be forced to provide data of their clients to governmental stakeholders or any other third party.
- The NREM should guarantee data protection standards and must secure the rights of the data subjects.
- The mandate and purpose of the NREM should be based on clear cooperation standards between NGO counselling centres and the NREM.
- NGO counselling centres should act as an autonomous stakeholder and must not be used as a data providing agency by respective governmental and intergovernmental stakeholders.
- NGO counselling centres should be trained by IT data protection experts to fully control their technical equipment and data base and to prevent unauthorised access by third parties.
- The NREM should have an independent status. Independency refers not only to be independent from the current governmental administration but it should also not being influenced by its respective other mandates and/or conflict of interests.

95 Privacy by Design means building in privacy right up front, directly into the design specifications and architecture of new systems and processes.

96 A Privacy Impact Assessment (PIA) is one of many tools used to help organisations ensure that the choices made in the design of a system or process meet the privacy needs of that system, typically by way of a directed set of questions, based on privacy requirements.

- The NREM should not have an operational role in the respective National Referral Mechanism[97].
- The NREM should be regularly monitored by the national data protection authority as well as by national human rights monitoring institutions.
- The NREM should collect data in a broader context than solely trafficking in human beings by including frameworks such as economic orders, exclusion, racism, border controls, de-regulation of labour etc.

5.2 Identification of trafficked persons and access to support structures

Challenge: registration and transfer of victims' personal data between countries of origin and destination and between national agencies;

datACT recommendations:

- Conducting Privacy Impact Assessments (PIA)
- Defining detailed purposes and time frame for collection of personal data and avoiding unnecessary transfer of personal data to the possible extent
- Maintaining and advocating for a decentralised and anonymous access services for trafficked persons.

Challenges of identification

Presumed trafficked persons are not always formally identified as victims of crime by authorities. This may be due to an irregular status, their reluctance to report the crime, or if investigations have been halted. Non-identification

97 „A National Referral Mechanism (NRM) is a co-operative framework through which state actors fulfil their obligations to protect and promote the human rights of trafficked persons, co-ordinating their efforts in a strategic partnership with civil society. The basic aims of a NRM are to ensure that the human rights of trafficked persons are respected and to provide an effective way to refer victims of trafficking to services. In addition, NRMs can work to help improve national policy and procedures on a broad range of victim-related issues such as residence and repatriation regulations, victim compensation, and witness protection. NRMs can establish national plans of action and can set benchmarks to assess whether goals are being met." (OSCE: National Referral Mechanisms – Joining efforts to protect the rights of trafficked persons, Warsaw, 2004, p. 15).

can have serious consequences for the presumed trafficked person, they may be denied their basic right to support and protection and often face detention because of their irregular residence status, and/or possible prosecution for crimes or public offences committed in the course of their trafficking experience.

One outcome of an authority's lack of recognition in allowing presumed victims access to support structures is an immense gap in official statistics on trafficking cases and statistical estimations produced international organization. For this reason governments and international stakeholders are increasing their political efforts, pushing for administrative procedures that would allow for the identification of victims. Within the Palermo Protocol, for example, there is no procedure on 'victim identification' set forth, and its only comment to this issue is a reference to advise states to "consider implementing measures to provide for the physical, psychological and social recovery of victims of trafficking in persons [...]"[98]. The Palermo Protocol does not define the circumstances under which a person may access support. The language of 'victim identification' has also been promoted on the UN level within the 'Recommended Principles and Guidelines on Human Rights and Human Trafficking'.[99] This document recommends States to develop guidelines for officials "to permit the rapid and accurate identification of trafficked persons". (Guideline 2, Art.1)

The EU Directive 2011/36/EU – adopted some 10 years after the Palermo Protocol – sets certain conditions to the access to support structures for presumed trafficked persons:

» Member States shall take the necessary measures to ensure that a person is provided with assistance and support as soon **as the competent authorities** have a reasonable-grounds indication for believing that the person might have been subjected to any of the offences referred to in Articles 2 and 3. (Art.11)

98 Palermo Protocol Art. 6 (3).

99 Office of the High Commission for Human Rights (E/2002/68/Add); http://www.ohchr.org/Documents/Publications/Traffickingen.pdf.

While victims of other violent crimes, including violence against women, are not obliged in European and international legislation to be identified by competent authorities in order to have access to support structures and protection, trafficked persons have to first convince officials about their status as a victim of a crime before receiving appropriate help.

The system of 'identification' as a qualification to access support structure poses challenges to privacy rights of presumed trafficked persons. As an example, when trafficked persons are confronted with an extensive bureaucratic access they have almost no opportunity to receive such services as counselling anonymously. Issues around identification procedures are also valid for victims who do not want to cooperate with law enforcement authorities in pursuing a criminal investigation process. The following two examples in this chapter will help to illustrate how suggested identification guidelines are primarily interested in the collection of personal and sensitive data of the 'to be indentified' presumed victim.

While European countries have different administrative and legal procedures intended for the 'identification' of trafficked persons, increasingly countries are collaborating in joint endeavours in order to harmonise victim identification systems on a regional level. In 2013, the European Commission (EC) launched a reference document on 'Guidelines for the identification of victims of trafficking in human beings, especially for Consular Services and Border Control'.[100] Referring to the 2012 EU Strategy, the EC highlights the importance of 'early identification' by providing a compilation of summaries from eleven EC funded projects on identification tools.[101] A central step in the EC guidelines for identification is the collection and processing of data by the competent authorities. It is in the EC guidelines for identification that we first see the recommended division of persons into two identities: the 'identified victim' and the 'potential victim'.[102]

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

101 See 'guidelines', p. 8–10.

102 See 'guidelines', p. 6.

Both concepts are included into the Eurostat statistics as well, however, the terminology is not consistent with the one from the EC guidelines for identification. The Eurostat reports refers to the term 'presumed victim' instead of 'potential victim':

» An 'identified victim' is defined as a person who has been formally identified as a victim of trafficking in human beings according to the relevant formal authority in Member States.

A 'presumed victim' of human trafficking is defined as a person who has met the criteria of EU regulations and international Conventions but has not been formally identified by the relevant authorities (police) as a trafficking victim or who has declined to be formally or legally identified as trafficked.[103]

As a consequence of these concepts, future EU efforts are targeted not only at identifying persons who fit into one of the two victim concepts, but also those persons do not want to cooperate with authorities or do not wish to be included into support structures.

In addition, cross-border procedures for the identification of victims were introduced through the concept of 'Transnational Referral Mechanisms' (TRMs) developed by the International Centre for Migration Policy Development (ICMPD).[104] Recently, the concept was also integrated into the 2012 EU Strategy:

The first recommended action under 'Identifying, protecting and assisting victims of trafficking' (2.1. PRIORITY A, Action 1) is the establishment of National and Transnational Referral Mechanisms which should describe procedures to better identify, refer, protect and assist victims and include all relevant public authorities and civil society by 2015.[105]

103 See http://ec.europa.eu/dgs/home-affairs/what-is-new/news/news/2013/docs/20130415_thb_stats_report_en.pdf, p. 26.

104 See ICMPD: Guidelines for the Development of a Transnational Referral Mechanism for Trafficked Persons in Europe: TRM-EU, 2010; http://www.icmpd.org/fileadmin/ICMPD-Website/ICMPD-Website_2011/Capacity_building/THB/Publications/TRM_EU_guidelines.pdf.

105 EU Strategy, p. 6.

The identification processes are based on intensive documentation and registration practices of presumed trafficked persons. In addition, the TRM recommends carrying out the 'formal identification' of trafficked persons by assigned authorities. 'Formal identification' by authorities is neither linked to a criminal investigation nor to the willingness of the victim to cooperate with law enforcement authorities. Once completed the 'formal identification' would allow the victim to access further services, including assistance, protection and social inclusion.[106] In the TRM Guidelines the ICMPD describes 6 measures in the identification process:

1. Initial screening and referral;
2. Access to basic needs and information;
3. Early risk assessment;
4. Language interpretation and cultural mediation;
5. Recovery and reflection period;
6. Identification.[107]

This model of identification may lead to serious data protection challenges for trafficked persons. For example, during the initial screening and early risk assessment, it recommends gathering information not only on the victims' personal data but also on his or her health issues.[108]

It is because of this privacy risk that the European Data Protection Supervisor (EDPS) has suggested that clear information be provided to individuals on how to benefit from the right to protection of personal data, as well as about the work of national data protection authorities should be part of national and transnational referral mechanisms.[109]

106 See ICMPD Guidelines for TRM, p. 56.

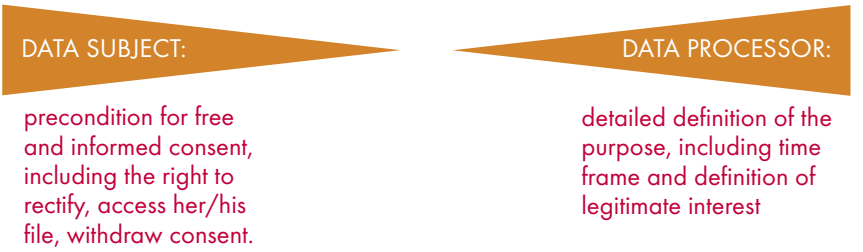
107 See ICMPD Guidelines for TRM, p. 34.

108 See ICMPD Guidelines for TRM, p. 43.

109 EDPS comments on the 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", p. 3; http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2012/12-07-10_Human_Trafficking_EN.pdf.

datACT recommendations

In general, anti-trafficking measures should clearly define the purpose of data collection once it is made a condition to access support structures. The purpose should be based on a legitimate interest. The processing of personal data is dependent upon the free and informed consent of the data subject, in this case the trafficked person. The following diagram illustrates the tension between the right of the data subject and the obligation of the data processor:



datACT recommendations of data collection for (NGO) service providers at initial counselling:

- The collection of trafficked persons' personal data should be minimised to the absolute necessary limit. The purpose of data collection should be deliberated and harmonised with existing European and national data protection provisions.
- Personal data that were collected for specific internal purposes should not be stored for any other purposes nor shared with external or other third parties: 'What is nice to have is not necessarily legitimate to have'.
- In cooperation with NGO service providers, indicators should be elaborated that define access for presumed trafficked persons to counselling centres.
- These indicators should neither overrule nor replace individual decisions of counsellors to accept presumed victims to support structures. The indicators are supposed to support the daily counselling practice.

- Presumed trafficked persons should have a low-threshold access to anonymous counselling. It is of paramount importance to establish a first contact to the presumed trafficked person in order to provide him/her with basic guidance on further steps.
- There is a need to establish reflection periods of at least three months in order to sustainably enable the presumed trafficked person to act in his/her best interest. The reflection period should aim at providing a safe space and sufficient time for presumed victims in order to consider the options and to make informed decisions.

datACT recommendations for return/social inclusion

- Any transfer of trafficked persons' personal data across national borders should be avoided.
- All stakeholders should have security measures in place to prevent tracing the identities of trafficked person after return and inclusion procedures.

5.3 Data protection and NGO service providers

Challenges: International IT case documentation and management system may not be secure; NGO counsellors may be put into a situation of sharing information with law enforcement; Victims' rights as data subject may not be an integral part of the counselling process.

datACT recommendation:

- Establishing secure IT soft- and hardware in NGO counselling centres based on a Privacy Impact Assessment (PIA);
- Advocating for stronger protection of the obligation to confidentiality and the right to refuse to give evidence in court;
- Introducing counselling modules on the right to privacy.

As discussed previously, NGO service providers may be put into a situation of sharing information about their clients, including personal data, with law enforcement, authorities or other stakeholders. Data sharing may occur during the counselling for the following reasons:

- Issuing a reflection delay and residence permit;
- Applying for social benefits;
- Reporting obligations to donors, including annual reports and statistics;
- Cooperation with the National Rapporteur and/or equivalent Mechanisms;
- Preparing for return and social inclusion measures in the country of origin;
- Other endeavours.

International, regional, and national political and legal instruments contain only vague descriptions on the structure and role of civil society cooperation with authorities regarding data collection and data protection. For this reason it is important that future guidelines advising NGOs on their role as data processors be elaborated and that their role is clarified in national and international data collection tools, such as the National Rapporteur and/or equivalent Mechanisms. The 2011 EU Directive recommends that civil society stakeholders seek cooperation with National Rapporteur Mechanisms but fails to define the role and mandate of NGOs in this context.

Flowing from the EU Directive 95/46/EC what follows is an example of Privacy Impact Assessment questions that will help to illustrate the need for clearly defined roles and obligations of NGO service providers regarding data protection provisions:

Article 6: Principles relating to data quality[110]

1. Member States shall provide that personal data must be:
   a) processed fairly and lawfully;

Questions for a PIA process for anti-trafficking Counselling centres[111]*:*

- Do presumed trafficked persons have the possibility for anonymous counselling at initial counselling?
- Have you established conditions for processing personal data of your clients (trafficked persons)?
- How will your clients (trafficked persons) be told about the use of their personal data?
- Do you need to amend your privacy notices?
- Have you established conditions and requirements for transferring personal data of your clients (trafficked persons)?
- Do you encode personal data of trafficked persons with an acronym or identification code?
- How do you organise internal consultations on cases?

   b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards;

Questions for a PIA process for anti-trafficking Counselling centres[112]*:*

- Have you discussed and identified the purpose for processing personal data?
- Have potential new purposes been identified as the scope of the project expands?

110 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data Official Journal L 281 , 23/11/1995, P. 0031–0050.

111 The questions are slightly adjusted from the UK data protection authority, the Information Commissioner's Office: Code of Practice: Conducting privacy impact assessments, February 2014, p. 39–41.

112 Ibid.

c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;

Questions for a PIA process for anti-trafficking Counselling centres[113]*:*

- Do you collect and process data in addition to the defined purpose?

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified;

Questions for a PIA process for anti-trafficking Counselling centres[114]*:*

- How are you ensuring that personal data could be corrected or deleted?

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use.

Questions for a PIA process for anti-trafficking Counselling centres[115]*:*

- How do you store personal data of your clients?
- What retention periods are suitable for the personal data you will be processing?
- Are you procuring software which will allow you to delete information in line with your retention periods?

2. It shall be for the controller to ensure that paragraph 1 is complied with.

113 Ibid.
114 Ibid.
115 Ibid.

Article 7: Criteria for making data processing legitimate

Member States shall provide that personal data may be processed only if:

a) The data subject has unambiguously given his consent; or
b) Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or
c) Processing is necessary for compliance with a legal obligation to which the controller is subject; or
d) Processing is necessary in order to protect the vital interest of the data subject; or
e) Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or
f) Processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1 (1).

Question for a PIA process for anti-trafficking Counselling centres[116]*:*

- Do you obtain informed consent of your clients (trafficked persons) during counselling?
- Do you inform your clients (trafficked persons) about the use and the storage of personal data?
- If you are relying on consent to process personal data, how will this be obtained and what will you do if it is withheld or withdrawn?
- Do you have agreements about data protection with authorities or third parties?

116 Ibid.

Article 1 (1) of the Data Protection Directive explains the scope of application:

» In accordance with this Directive; Member States shall protect the fundamental rights and freedoms of natural persons and in particular their right to privacy with respect to the processing of personal data.

Questions for a PIA process for anti-trafficking Counselling centres[117]*:*

- Does your IT experts and technical data base manager have access to the personal data?
- Will you be required in the framework of return programs and international cooperation to transfer data outside your country and outside of Europe?
- Do you transfer personal data within the framework of international organisations and return programs?
- If you will be making transfers, how will you ensure that the data is adequately protected?
- Do you provide your client (trafficked person) with contact details of the person in charge to address him or her access request in your organisation?
- Did your counselling centre already establish cooperation with the relevant Data Protection Authority?
- Are you legally obliged to appoint a data protection officer within your organisation?

117 Ibid.

datACT recommendations

- Legal rights for presumed trafficked persons as data subjects should be an integrated part of standard counselling.
- Presumed trafficked persons should be informed at all stages about the use and storage of data related to their respective case.
- All European NGO service providers should be granted the right to refuse to give evidence to law enforcement/judicial authorities.
- Internal consultations on cases should be verbal and written documentation should be discouraged.
- NGOs should advocate for an absolute minimum of data collection of the personal data of presumed trafficked persons by governmental and intergovernmental organisations and monitor this to promote compliance.

ANNEX I

CATALOGUE OF RIGHTS OF DATA SUBJECTS TO BE INTEGRATED INTO NGO COUNSELLING

WHAT ARE YOUR RIGHTS?

General right

Individuals are safeguarded by a general right to have their personal data processed fairly and lawfully, and only for legitimate purposes.

Specific rights

This general right is complemented by a number of specific rights of the individual, including the:

- Right to know if an institution or a body is processing data concerning him/her;
- Right to information about the particular processing (what information is being processed);
- Right to object to the processing on compelling and legitimate grounds;
- Right to be informed with information such as the identity of the controller, the purpose of the processing, the recipients of the data;
- Right to access to his/her personal data;
- Right to rectify inaccurate, out-of-date or incomplete data;
- Right to block data whose accuracy is contested;
- Right to erasure of data if the processing is unlawful;
- Right to notification of any deletion, rectification or blocking of his/her data to a third party to whom the data have been disclosed;
- Right to object to such disclosure;
- Right to compensation for any damages.

What are your responsibilities in protecting your personal data?

- Think before disclosing your information;
- Only disclose information that is needed by the organisation involved;
- Question why someone might ask for your particular personal information.

ANNEX II

DATA PROTECTION STANDARDS FOR NGO SERVICE PROVIDERS

The datACT standards were developed and discussed during numerous consultations with anti-trafficking NGO service providers between 2013–2014, including during regular KOK alliances meetings, La Strada International NGO platform meetings in Talinn, Estonia and in Sofia, Bulgaria and during a workshop at the Global Alliance against Trafficking in Women (GAATW) International Members' Congress in Bangkok, Thailand.

The purpose of the standards is to provide guidance to anti-trafficking NGOs, including counselling centres to protect privacy rights of trafficked persons.

It aims at establishing a framework for NGOs to evaluate, monitor and initiate data protection in daily counselling work, as well as for the purpose of developing a long-term data protection strategy. The standards are a 'living document' and open for feedback by practitioners.

1. Basic principles of data collection for (NGO) service providers at initial counselling/'identification'

- The collection of trafficked persons' personal data should be limited to the absolute necessary minimum. The purpose of data collection should be deliberated and harmonised with existing European and national data protection provisions.

- Personal data that were collected for specific internal purposes should not be stored for any other purposes nor shared with external or other third parties. ('What is nice to have is not necessarily legitimate to have')

- Indicators should be elaborated in cooperation with NGO service providers defining access to counselling centres for presumed trafficked persons.

- These indicators should neither overrule nor replace counsellors' individual decisions to accept presumed victims to support structures. The indicators are intended for the support of daily counselling practice.

- Presumed trafficked persons should have a low-threshold access to anonymous counselling. It is of paramount importance to establish a first contact with the presumed trafficked person in order to provide him/her with basic guidance to the possible next steps.

- There is a need to establish reflection periods of at least three months in order to sustainably enable the presumed trafficked person to act in his/her best interest. The reflection period should aim at providing a safe space and sufficient time for presumed victims so that they may consider their options and make informed decisions. This reflection period should be granted irrespective of their willingness to cooperate with law enforcement authorities.

2. Data protection and data collection for (NGO) service providers during comprehensive counselling

- NGOs should advocate and monitor that data collection of victims' personal data by governmental/intergovernmental organisations be reduced to the absolute minimum.
- Personal data should be encoded with an acronym or identification code by the NGO service providers.
- NGOs should develop and install secure soft- and hardware for their case management system with the support of ICT data protection experts. Cloud computing and data storage services, and remote access to client data should be avoided.
- All cooperation with authorities or third parties should be based on the agreement that all data used be strictly anonymised data.
- NGO service providers should obtain the right to refuse to provide client information or other evidence to judicial authorities.[1]

1 OSCE NRM

- Internal consultations on cases should be verbal and written documentation should be discouraged.
- The purpose of collecting and storing the trafficked person's personal data should be clearly defined, including timeframes for retention and the date of termination of stored personal data.
- Only designated staff members should have access to the files containing personal data of trafficked persons.
- All data collection efforts should be based on data protection methods, such as 'Privacy by Design'[2] and 'Privacy Impact Assessments'[3].

2 Privacy by Design means building in privacy right up front, directly into the design specifications and architecture of new systems and processes.

3 A Privacy Impact Assessment (PIA) is one of many tools used to help organisations ensure that the choices made in the design of a system or process meet the privacy needs of that system, typically by way of a directed set of questions, based on privacy requirements.

3. Information on data protection for trafficked persons by service providers

- Legal rights for presumed trafficked persons as data subjects should be an integrated part of standard counselling.
- Presumed trafficked persons should be informed at all stages about the use and storage of data related to their respective case.
- Presumed trafficked persons should give their informed written consent before collecting their personal data.
- NGO service providers should assign a staff member to be the contact person for trafficked persons in the event they want to withdraw their consent, or to access or rectify their data.

4. Data protection and return/social inclusion

- Any transfer of trafficked persons' personal data across national borders should be avoided.
- It should be secured by all stakeholders that identities of trafficked persons can not be traced during and after return and inclusion procedures.

5. National Reporting and/or Equivalent Mechanisms (NREM)

- The NREM should guarantee data protection standards and must secure the rights of the data subjects.
- The protection of the trafficked persons' privacy should be at the core of all data collection measures.
- All data collection efforts should be based on data protection methods, such as 'Privacy by Design'[4] and 'Privacy Impact Assessments'[5].
- NGO counselling centres should not be forced to provide data of their clients to governmental stakeholders or any other third party.
- The mandate and purpose of the NREM should be based on clear cooperation standards between NGO counselling centres and the NREM.
- NGO counselling centres should act as an autonomous stakeholder and must not be used as a data providing agency by respective governmental and intergovernmental stakeholders.

4 Privacy by Design means building in privacy right up front, directly into the design specifications and architecture of new systems and processes.

5 A Privacy Impact Assessment (PIA) is one of many tools used to help organisations ensure that the choices made in the design of a system or process meet the privacy needs of that system, typically by way of a directed set of questions, based on privacy requirements.

- NGO counselling centres should be trained by ICT data protection experts to fully control their technical equipment and data base and to prevent unauthorised access by third parties.

- The NREM should have an independent status. This refers not only to be independent from the current governmental administration but also from not being influenced by inter-organisational mandates and/or conflict of interests.

- The NREM should be monitored regularly by the National Data Protection Authority and National Human Rights Institution.

- The NREM should not have an operational role in the respective National Referral Mechanism.

- The NREM should collect data in a broader context than solely trafficking in human beings by including frameworks such as economic orders, exclusion, racism, border controls, de-regulation of labour etc.

REFERENCES FROM THE PROLOGUE

Amnesty International (2013) Scotland's Slaves. An Amnesty International briefing on trafficking in Scotland 2013 [cited 20 September 2013]. Available from 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 no. 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 no. 33 (2):251-277.

ASTRA Anti-Trafficking Action (2013) Human Trafficking – Manual for Journalists 2009 [cited 18 September 2013]. Available from 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 [cited 20 September 2013]. Available from http://ec.europa.eu/anti-trafficking/EU+Policy/Report_DGHome_Eurostat.

Frontex (2013) Situational Overview on Trafficking in Human Beings 2011 [cited 20 September 2013]. Available from 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 [cited 22 June 2007]. Available from http://www.icmpd.org/829.html.

Laczko, F. (2002) 'Human trafficking: the need for better data.' Migration Information Source no. 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 [cited 14 September 2013]. Available from 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 no. 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 [cited 20 September 2013]. Available from http://www.unodc.org/unodc/en/human-trafficking/2009/anti-human-trafficking-manual.html.

UNODC (2013) Global Report on Human Trafficking. UN.GIFT 2009b [cited 18 September 2013]. Available from 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 no. 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.

SELECTED REFERENCES

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

European Convention on Human Rights (ECHR) 1950.

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, Niemietz 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.

ICMPD, Guidelines for the Development of a Transnational Referral Mechanism for Trafficked Persons in Europe: TRM-EU, Vienna 2010.

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 Forced 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.datact-project.org

KOK

German NGO Network against Trafficking in Human Beings

www.kok-gegen-menschenhandel.de

Project Partner:

La Strada INTERNATIONAL

www.lastradainternational.org