Humanitarian Passport
Feasibility Study

FINAL 12-2-2019

Dutch Relief Alliance[1]

February 2019

[1] This report was prepared by Anne Janssen and Caroline Scheffer. Any opinions expressed in this report are those of the authors and do not necessarily reflect the position of individual Dutch Relief Alliance members.

Table of Contents

1. Introduction 3

2. Existing/expected integrity screening instruments 4

2.1 What needs to be addressed by an integrity screening system? 4

2.2 Which integrity screening instruments are in place for the sector as a whole? 5

2.3 Which gaps remain? 7

3. Findings research on potential other instruments 7

3.1 Persons Register Child Care Netherlands 8

3.2 Emergency Response Rosters 9

3.3 Black List 9

3.4 United Nations Misconduct Tracking System 12

3.5 Inter-Agency Misconduct Disclosure Scheme 12

3.6 INTERPOL pilot 'Operation Soteria' 13

3.7 Digital ID System 13

4. Conclusions and Recommendations 14

4.1 Conclusions 14

4.2 Recommendations 16

Abbreviations

AP	Data Protection Supervisor (*Autoriteit Persoonsgegevens)*
BCR	Binding Corporate Rules
DPIA	Data Protection Impact Assessment
DRA	Dutch Relief Alliance
DUO	*Dienst Uitvoering Onderwijs*
EU	European Union
GDPR	EU General Data Protection Regulation
GGD	*Gemeentelijke of Gezamenlijke Gezondheidsdienst*
HR	Human Resources
MIVD	Military Intelligence and Security Service *(Militaire Inlichtingen- en Veiligheidsdienst)*
MoD	Ministry of Defence
MTS	Misconduct Tracking System
SCC	Standard Contractual Clause
SEA	Sexual Exploitation and Abuse
UK	United Kingdom
UN	United Nations
VOG	Declaration of Good Conduct (*Verklaring Omtrent Gedrag)*

1. Introduction

Following the reports of sexually transgressive behaviour and abuse of power by some staff members of international aid organizations, a broad coalition of organisations in the sector in the Netherlands developed a Joint Integrity Action Plan[2] (hereinafter: Action Plan). The purpose of this Action Plan is to improve the prevention, signalling, enforcement and accountability of (sexually) transgressive behaviour and abuse of power in the sector. The projects of the Action Plan are organized around the following four action lines:

I. Improve integrity systems
II. Take preventive measures
III. Report safely and act appropriately
IV. Transparent accountability

The humanitarian and development sector (hereafter: the sector) recognises that more needs to be done to ensure the right people are in the right places. By better vetting of personnel and ensuring that only staff with clean records are being sent for humanitarian operations, the sector aims to prevent (sexual) misconduct and abuse as well as rebuild, regain and maintain the trust of the general public and donor community. Strengthening of screening systems is only one action that is being taken to prevent (sexual) misconduct and abuse and more will need to be done to bring about a cultural change across the sector which is addressed to an extent by other projects of the Action Plan, but requires continuous attention of individual organisations.

In March 2018, an Integrity Task Force was established by the Dutch Relief Alliance (DRA)[3] with four key roles and responsibilities:

1. Draft minimum standards of Integrity Policy DRA-members;
2. Establish reporting procedure within the integrity policy;
3. Capacity building on integrity policy, prevention of sexual exploitation and abuse, and the Core Humanitarian Standards;
4. Look into the possibilities of developing a humanitarian passport/ a personal certification system.

The DRA, initially cooperated with the Dutch Coalition for Humanitarian Innovation (DCHI) to look into the possibilities of a ''humanitarian passport". This feasibility study aims "to understand the barriers and opportunities for identifying a solution and establishing a system which prevents persons who have been convicted of (sexual) misconduct to enter into employment elsewhere in the sector". A key focus is to explore the feasibility of a solution that provides Human Resources staff with necessary information to make an informed decision about recruitment of new personnel and prevent recruitment of someone who has committed misconduct.

In addition to better vetting, with the technical support of DCHI, the DRA has undertaken several steps based on these agreements starting with an exploration phase to define the problem statement, set the scope, and identify core functions, bottlenecks and core questions. To this end, a survey was shared among DRA members to determine current practices around recruiting and vetting of new employees. The survey found that the ultimate objective of an integrity screening system is to protect vulnerable populations from personnel that can misbehave and/or break the code of conduct and prevent someone who has been responsible for abuse in the past from securing employment in the sector

[2] https://www.partos.nl/fileadmin/files/Documents/Actieplan_Integriteit_def.pdf

elsewhere. Consequently the "humanitarian passport initiative" was split into two parallel – but closely linked – processes whereby, on the one hand, a 'Roadmap Screening' was developed (see chapter 2) and, on the other hand, a study is conducted to explore the feasibility of a sector-wide black list or "humanitarian passport" by looking at experiences from other organisations who have implemented professional registers or other instruments to prevent and address (sexual) misconduct both in The Netherlands and abroad.

This report presents the main findings of the research into potential instruments that could be implemented to increase sharing of information related to (sexual) misconduct during the recruitment stage, with a focus on the black list and so-called "humanitarian passport". It includes experiences from other sectors in The Netherlands, such as the child care sector and the Ministry of Defence, as well as measures that are already in place or are being developed by other humanitarian and development organisations. The report starts with a description of existing integrity instruments to determine what aspects of the problem statement are being addressed already and which gaps still remain. The next chapter will look into other instruments that could be implemented and the experiences of other organisations/agencies. Finally, after the concluding remarks, key recommendations will be presented to inform potential next steps in strengthening the integrity screening system within the sector.

2. Existing/expected integrity screening instruments

This section briefly presents the problem statement and the key results of the DRA survey to determine what issues an integrity screening system should address, as well as the Roadmap Screening in order to identify the gaps that remain to be addressed.

2.1 *What needs to be addressed by an integrity screening system?*

As noted in the introduction section, an integrity screening system should be able to identify candidates which have a previous record of (sexual) misconduct and/or abuse of power upon entry into a humanitarian or development organisation. Furthermore, it should allow for sharing of information to ensure that employers can make an informed decision when recruiting new personnel and prevent someone who has been responsible for (sexual) misconduct in the past from securing employment elsewhere in the sector. Ultimate responsibility for recruitment will remain with the individual organisations.

Ideally, a system would at a minimum need to include the following information:

- Name, summary of background, experience in humanitarian and development work
- Information about breaches of code of conduct, including (if applicable):
    - Proof of abuse of power and SEA towards beneficiaries and staff members (SEA reports which are to be proven reliable and valid; "*Verklaring Omtrent Gedrag*"/Criminal records).
    - Information about previous suspensions or dismissal as a result of misconduct
    - Inappropriate disclosure of confidential information related to beneficiaries and staff

Based on the DRA survey, the following core conditions for any system were identified:

- Provide transparent, authentic and reliable background information of an employee, though only data that is needed at a minimum
- An objective source should determine the content of the register
- Protected database meeting privacy law (GDPR)/ legal requirements globally (ensuring it is lawful for all countries)

- Accessible globally and between agencies (humanitarian and development organisations)
- Highly confidential; only accessible for HR Directors of organizations which are registered
- Should carefully deal with wrongful and/or unjustified accusations so there should be high standards before any information can be shared in the system
- Quick access to and updating of data/information to ensure it is user-friendly and error sensitive

2.2 *Which integrity screening instruments are in place for the sector as a whole?*

Every organisation has their own recruitment system, Code of Conduct and policies to safeguard and protect its beneficiaries and staff. This is also where the challenge lies as there is no uniform policy across the sector to screen new personnel, especially against records of previous misconduct.

Over the past months, a project group led by The Netherlands Red Cross – in cooperation with the DRA and with legal support from Hunter Management Partners – has developed a 'Roadmap Screening'[4] to improve and standardise the screening process within the humanitarian and development sector in The Netherlands and, at the same time, send a clear preventative signal to potential employees and the public that misconduct is taken seriously.

The screening process is meant to give employers information about a candidate in order to make an assessment about their integrity before hiring someone. There are a number of general requirements that need to be met in order to screen potential employees. These include:

a. A justifiable interest for necessity of screening
b. A careful consideration of the job groups to which the screening applies
c. Only information relevant to a function can be collected
d. The screening period
e. Informing a potential employee about the screening results
f. Alignment with privacy law (General Data Protection Regulation – GDPR[5])
g. Data retention period when someone does not proceed in recruitment procedure
h. Data retention period upon employment
i. Data retention during employment

The project team developed five instruments:

I. <u>Announcement screening procedure</u>

- *Why?* A potential employee needs to provide permission for the screening. If this is only sought during the selection process, the candidate is in a dependent position and may feel pressure to provide permission.
- *When?* Before the selection process is started.
- *What?* An organisation should announce the screening procedure on its website as well as in the vacancy notice to inform potential employees and ensure they agree with the screening prior to applying for the job. Sample announcement texts are provided in the Roadmap Screening.

[4] The Roadmap Screening is currently only available in Dutch and can be found on the website of Partos along with other results of the Action Plan.
[5] In The Netherlands, the GDPR is known as the *Algemene verordening gegevensbescherming (AVG)* and is in place since 25 May 2018.

II. Self-declaration of good behaviour and application form

- *Why?* The self-declaration and application form will give employers a stronger position to terminate an employment contract if information about misconduct only surfaces once an employee is hired.
- *When?* A self-declaration form is sent along with the application form via email to the candidate prior to the first interview and returns signed copies during the first interview.
- *What?* A self-declaration is understood to mean "a self-declaration of good behaviour". It is a statement drawn up by the organization, whereby the potential employee declares to have not been in touch with the police and judicial authorities or is otherwise involved in integrity issues. Templates for the self-declaration and application form are attached to the Roadmap Screening.

III. Reference Checks

- *Why?* The reference check is meant to give employers more information about previous functioning of a candidate, including information about their integrity.
- *When?* Reference checks should be completed by the time a job offer is made to the candidate.
- *What?* A double reference check is highly recommended whereby a reference is requested from the last and the penultimate employer. The reference should be provided in writing by a line manager (or HR director who has access to the potential employee's professional file) and signed by the person giving the reference. A checklist for HR about the reference check, a reference check template, as well as the Inter-Agency Misconduct Disclosure Scheme[6] is attached to the Roadmap Screening.

IV. "Verklaring Omtrent Gedrag" (VOG - Certificate of Conduct)

- *Why?* A Certificate of Conduct (VOG) is a document by which the Dutch State Secretary for Justice and Security declares that the applicant did not commit any criminal offences that are relevant to the performance of his or her duties.
- *When?* The VOG should be applied for either after a positive first interview or after conducting the reference checks. Since it can take up to 4-8 weeks for a Certificate of Conduct to be issued, a termination clause should be incorporated in a contract in case of non-issuance. It is recommended that a VOG is requested every three years.
- *What?* An employee requests a VOG, which is facilitated by the employer who provides relevant information. In the system a consideration is made whether criminal offenses (might) constitute an obstacle to the issuance of the VOG, based on a general or specific screening profile. This is done based on one or more of the eight risk areas (Information, Money, Goods, Services, Business transactions, Processes, Organisation management, Persons). Since the VOG is specific to the Dutch context, the Roadmap Screening also provides recommendations for steps to take in case of persons without Dutch nationality residing abroad or Dutch nationals who have resided abroad for an extended period. At the time of writing, no VOG profile exists which covers criminal offences relevant to humanitarian and development settings (child abuse, abuse of power, sexual abuse and/or financial abuse), but the project team is conducting further research and a report will follow.

[6] https://interagencystandingcommittee.org/system/files/inter-agency_misconduct_disclosure_scheme_final_draft_002.pdf

V. **Checklist recruiting integer staff**
   - *What?* A checklist including all steps to take during the screening procedure is attached to the Roadmap Screening.

2.3 *Which gaps remain?*

While the screening process actions as described above are a big step forward in standardising and improving the recruitment processes of humanitarian and development organisations in The Netherlands, it does not address all the issues an integrity system is meant to address. As mentioned earlier, there are two key objectives of the system:

1. Identify candidates with a previous record of (sexual) misconduct and/or abuse of power.
2. Allow for sharing of and quick access to information to ensure that organisations recruiting new personnel can make an informed decision and include information related to misbehaviour and/or breaches of a Code of Conduct in the recruitment decision-making process.

The Roadmap Screening as briefly described above will address the first objective of an integrity system, whereby the three instruments of a self-declaration, reference checks and VOG are meant to identify and prevent the hiring of someone with a previous record of (sexual) misconduct and/or abuse of power. It should be noted though that this screening process does not provide easy and quick access to information important for recruitment for quick deployments in case of emergencies nor will it have a whistleblowing function. The second objective is being addressed to a certain extent as information on integrity and misconduct is shared through reference checks, but there is no central location where this kind of information is stored and accessible. Furthermore, the Roadmap Screening has mainly been developed for the Dutch context and while it includes some recommendations for international information sharing, the VOG is a Dutch instrument. The link with international developments, such as the INTERPOL pilot project to strengthen criminal record checks and information sharing (see section 3.5), is therefore particularly important.

Different instruments could potentially be introduced in order to (partially) address these remaining gaps, including a persons register or black list. As these instruments are not common practice yet in the humanitarian and development sector, meetings were held with experts from other sectors as well as humanitarian and development organisations in The Netherlands and abroad to learn from their experiences with these instruments. The next section will present the results of this exploration.

3. Findings research on potential other instruments

Before going into the findings, it is important to determine what exactly a “humanitarian passport” entails as the term has been widely used within and outside of The Netherlands without specifying what it looks like. Ultimately, it is a sort of clearance that shows someone is honest and reliable, does not have serious integrity notes in their personnel file and has never come into contact with the law because of misconduct and abuse. The screening procedures as described above will, in principle, provide employers with this type of information. The main gaps that remain after these screening procedures are thus the access to information regarding integrity in one central place to enable swift checking before recruitment as well as international information sharing especially related to the VOG. A persons register and black list have been named as two instruments that could address this gap,

which will be elaborated below. There are also several international screening-related integrity instruments which are already in use or under development that will be briefly explored.

3.1 *Persons Register Child Care Netherlands*

The child care sector in The Netherlands introduced a continuous screening of employees in 2013. This meant that everyone who is employed in the child care sector needs to have a VOG which is automatically checked by the Ministry of Justice and Security (Justis), on a daily basis. This system however did not screen volunteers, interns or consultants engaged at child care facilities, especially at host family facilities. Therefore, an obligatory registration in a persons register was introduced in March 2018 to ensure everyone who regularly comes into contact with children, including non-personnel, in child care is continuously screened. The system mainly has a deterrent function but has also the ability to identify people who have committed a criminal offence prohibiting them to work in the child care sector.

This system is grounded in Dutch sector-specific law and regulations and meets strict conditions, including related to privacy legislation. The register is a chain of actors that are interconnected and who have (restricted) access based on their responsibility. The continuous screening is done by Justis for all persons registered in the system who checks daily if someone's VOG is accepted or rejected. Any signal related to someone's VOG is passed to the *"Dienst Uitvoering Onderwijs" (DUO).* DUO maintains the register and deals with any signals coming from the continuous screening by sharing them with the *"Gemeentelijke of Gemeenschappelijke Gezondheidsdienst"* (GGD). The GGD, in turn, uses the register during inspections of child care locations to ensure everyone who is present on a structural basis is also registered and investigates any signal received from DUO. Finally, the child care facilities themselves are responsible for ensuring that everyone is registered.

While the continuous screening ensures that any new record in the justice system is immediately picked up, the information contained within this system is limited as only information about a person's VOG acceptance or rejection is shared among these actors. The information is saved in a secure manner with a strict division of roles for who has access to personal information. No other information is recorded in the system and details about a VOG rejection are only known by Justis and the individual involved.

Challenges

The register has some limitations, most notably regarding the lack of registration of cases whereby no official record is present in the criminal justice system. References therefore remain a very important aspect of selection and screening in order to get more information about misconduct that does not break any national legislation and as such would not show up in someone's VOG, but for instance does break an organisation's Code of Conduct.

It should be noted that the register as used within the child care sector in The Netherlands is based on sector-based legislation and regulation which is not yet available for the humanitarian and development sector. Finally, it is very costly to develop such a register and it lacks some information which DRA members indicated should be part of an integrity screening system, such as references, a person's background and work experience as well as the international sharing of information.

3.2 *Emergency Response Rosters*

Most humanitarian organizations have emergency response rosters including vetted individuals that can rapidly be deployed for emergencies. In many cases the organization's global information networks carry out international and domestic background checks for international employees or employees who have lived outside of the country (where the roster is managed) in the last 5 years. Global information checks are carried out for all employees. The information then stored on the roster includes information on past employment, employees' curriculum vitaes, contact details, address, salary expectations, jobs applied for previously, previous employers and concerns on (child) safeguarding. As data can only be stored for one year, the interagency approach, the "Interagency Misconduct Disclosure Scheme" (see also section 5.3) will ensure more accurate information on safeguarding concerns. References are in many cases updated on a regular (yearly) basis.
Within the organization the HR departments have access to the global roster who will share potential employees with country offices upon the request of rapid deployments. In line with GDPR, roster member details are not shared without their permission. If individuals do not receive positive references from in-country managers or if concerns are flagged, measures will be taken in line with the organization's protocol. This includes removal from the roster with immediate effect. Whilst such rosters provide a useful tool for rapid deployments within organizations, the information is only stored in the roster for one year and cannot be shared with external organizations.

3.3 *Black List*

The term black list is used to describe a list or registration of unwanted/unsuitable persons for an organization, sector, function or task. The purpose of a black list is to warn organisations/businesses about certain people and often contain criminal data or data about undesirable behaviour. In The Netherlands, there are strict conditions attached to a black list because of its nature, which include: 1) an organisation must have a legitimate interest; 2) the black list must be essential. In other words, the information cannot be gathered in a less invasive manner; and 3) the business interest must outweigh a person's privacy. If these conditions are met, a black list may be used within an organisation in The Netherlands and the European Union (EU).

There are already organisations in The Netherlands working with a black list, such as Oxfam and the Ministry of Defence (MoD). The way in which these lists are used are described below, but it should be noted that these are all lists used within the respective organisation.

Oxfam
Among other integrity measures, Oxfam is developing internal protocols for creating a robust recruitment screening process that takes safeguarding and integrity considerations into account. As a first step, Oxfam has devised a system to ensure that all references from Oxfam come from an accredited referee (such as HR Directors). To ensure staff who have faced disciplinary action, including for gross misconduct such as fraud, sexual exploitation and abuse, or abuse of power, cannot move undetected from one affiliate to another or within the sector, this centralised referencing process incorporates relevant disciplinary action in the reference (subject to, and where permissible under, applicable legal and regulatory requirements).

Ministry of Defence

Integrity violations within MoD are managed in a decentral manner by each of the seven organisational elements[7] who include violations in individual personnel files. This information should also be transferred to the central personnel system where it can be accessed by certain staff in case someone moves functions between organisational elements. Information related to integrity may not always be included in the central personnel system for different reasons, however the information from a personnel file will always come forward during screenings by the Military Intelligence and Security Service (MIVD). Almost everyone employed at MoD is screened by the MIVD upon entry, with a renewed screening every 5 to 10 years and/or when a substantial change in a life situation, such as a marriage, takes place. The extent to which a person is screened depends on the specific function level (e.g. corporal) they will fulfil.

Possibilities for sharing a black list

Challenges related to the implementation and use of a black list are generally shared by different organisations and are mainly related to information sharing restrictions resulting from privacy legislation. Before assessing the added value and concerns related to a sector-wide black list in addition to the Roadmap Screening, the possibilities for sharing a black list are thus explored.

A black list can normally only be used internally within one organisation because of the risks associated with sharing a list with privacy sensitive information. To share a black list between organisations in a sector within The Netherlands, authorisation from the Personal Data Supervisor (AP) is required. The AP will assess if sharing of the black list follows the conditions as set out in the GDPR[8]. To request this authorisation, several documents need to be provided along with the application form:

- A Data Protection Impact Assessment (DPIA) describing issues related to the intended data processing, identification of any privacy risks for those involved and the measures taken to limit these risks. How and with whom information is shared outside of The Netherlands should be described as specific as possible in the application form. Which additional steps are taken to ensure sufficient data protection in case of data sharing and processing outside of The Netherlands/EU should be included in the DPIA.
- If the DPIA determines there is a high privacy risk, and there are not enough measures in place to reduce these risks, a prior consultation with the AP needs to be requested as well.
- A protocol describing how personal data will be processed and how this data processing complies with privacy legislation requirements. An instruction manual[9] exists outlining requirements of the protocol, including general requirements, verifiable criteria for including someone on a black list, as well as safeguards for processing of personal data and safeguards for those involved. It should be noted that criteria related to aggravated behaviour rather than criminal offenses can only be included if these are socially unacceptable and stem from, for instance, a Code of Conduct.

For sharing of a black list outside of The Netherlands, additional steps are required, depending on whether the information is shared inside or outside of EU countries and if the country has an adequate

[7] Royal Netherlands Army, -Navy, -Air Force, -Marechaussee, Joint Support Command, Defence Material Organisation and Central Staff.

[8] According to Article 4:13, paragraph 2 of the General Administrative Law Act (*Algemene Wet Bestuursrecht)* a decision should be issued within eight weeks, or a reasonable period has to be provided if this timeframe cannot be met.

[9] https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/avg-handleiding_protocol_zwarte_lijst.pdf

level of data protection[10]. All EU countries are one jurisdiction when it comes to the protection of personal data as the level of data protection is equal across all EU countries. Therefore, if information is shared with a participating organisation in another EU country (including Norway, Liechtenstein and Iceland), that organisation only needs to meet the conditions set forth in the GDPR. There are different options for sharing of information outside the EU. Binding Corporate Rules (BCR) could be drawn up in line with the GDPR if information from the black list is to be shared within an organisation's office outside the EU. The BCR will also have to be approved by European Data Protection Supervisors as well as the European Data Protection Board. This approval process may take up to a year or longer. Alternatively, Standard Contractual Clauses (SCC) could be signed between two organisations whereby one organisation is based within the EU and one outside. If no changes are made to the SCC, no authorisation from the AP is required, but if changes are made authorisation from the AP must be received.

Added value and concerns of a shared black list

As noted above, the Roadmap Screening already covers the proposed objectives of an integrity screening system to a certain extent. The main gap identified relates to the screening for recruitment for quick deployments in case of emergencies as the screening can take quite some time, especially if a VOG or criminal background check from a third country needs to be requested. A sector-wide black list could partially cover this gap as organisations will be able to more quickly and pro-actively screen people against a central database of persons whose previous misconduct track record would prevent them from being deployed during an emergency. Sharing of information on the black list is in principle also possible outside The Netherlands, provided that the receiving organisation meets the requirement of the GDPR and a SCC or BCR are in place. It would however still require organisations to verify a candidate's background and work experience. A shared black list is thus only one of the instruments to enhance screening, but with the right authorisations in place, it will facilitate sharing of integrity-related information from a black list.

There are also several reasons why a black list would be preferred over a persons register, most notably:

- The main objectives of an integrity screening system are to identify candidates which have a previous record of (sexual) misconduct and/or abuse of power and share this information among organisations in the sector to make an informed recruitment decision. A persons register would include information about all persons employed by an organisation, a black list only about those persons who have committed misconduct. A black list would thus be more in line with the objectives as identified previously by DRA members.
- A black list encompasses less personal data which makes the system clearer and more concise, though the criminal data brings additional privacy risks.
- A black list has a lower administrative burden than a persons register.
- It is easier to bring about a shared black list through the AP than it is to develop a persons register which requires sector-based legislation and regulation.

There are nevertheless a number of concerns associated with developing and sharing a black list across the sector. While some of these will be addressed by a protocol, an agreement on these issues would first have to be found among organisations wishing to participate in sharing a black list. For instance, criteria not related to criminal offenses must be unambiguous and based on a Code of Conduct (or similar document). At the moment, there is no sector-wide Code of Conduct that could be used for

[10] The European Commission decision on countries with an adequate level of data protection can be found here.

this. Moreover, one organisation or authority would have to be identified who will be responsible for developing the required documents needed for the authorisation process as well as –later on – managing the shared black list in line with the GDPR. Finally, concerns have been raised during feedback rounds related to the proportionality of criteria for inclusion on a black list. Verifiable criteria will have to be drafted for the protocol, which should be careful not to 'sentence someone for life' yet also not be limited to criminal offenses only. The criteria will thus have to be carefully weighed taking into consideration the protection and rights of beneficiaries and staff on the one hand and the rights of those persons with proven (sexual) misconduct and abuse allegations.

3.4 *United Nations Misconduct Tracking System*

The Conduct and Discipline Unit manages a Misconduct Tracking System (MTS) which is a restricted-access database used, in part, for vetting of candidates for United Nations (UN) Field Missions "against records of prior misconduct while in the service of a UN Operation"[11]. The MTS was designed as a system to keep track of allegations from the point when it was received until the point when all required actions are taken. The MTS thus contains a vast amount of data and case-related correspondence, including information regarding victims and perpetrators, as well as results from the investigations and accountability measures taken following substantiated allegations. The main purpose is thus to keep a record and track actions taken in addressing data of allegations of misconduct. Data, extracted from MTS and other sources, on sexual exploitation and abuse and other misconduct, can be found on their website. However, the MTS is also used as part of the vetting process conducted at the time of recruitment, whether to verify manually or through electronic exchanges of information to check if there is a possible match against lists for deployment of deploying personnel. In the latter case, the system will be triggered if there is a match which will be manually verified. A match made through manual verifications will be shared with the recruiting entity.

Currently, MTS is used in screening personnel, civilian and uniformed, deploying to UN field missions only. However, data from the MTS on substantiated cases of sexual exploitation and abuse, as well as on sexual harassment, will be included in the vetting database that is being developed by the Office of the Special Coordinator. This database on sexual exploitation and abuse is being developed for the purpose of vetting only and as such will not include as much information as the MTS, but is meant to be shared across UN agencies, funds, programmes and the Secretariat. For the time being, NGOs will not have access to this database.

3.5 *Inter-Agency Misconduct Disclosure Scheme*

During the Safeguarding Summit in London on 18 October 2018, a new Inter-Agency Misconduct Disclosure Scheme was presented to which organisations can sign up. The purpose of the scheme is "to establish a minimum standard for humanitarian, development and other civil society organisations to share information as part of their recruitment process about people who have been found to have committed sexual harassment, sexual abuse or sexual exploitation during employment"[12]. The scheme is designed as a complementary tool for organisations to use during their existing recruitment processes and is a general tool to be adapted to internal policies and national privacy laws and regulations. At the moment, misconduct is limited to sexual harassment, - abuse, and - exploitation, but this definition may be broadened in time.

[11] https://conduct.unmissions.org/prevention-vetting
[12] Inter-Agency Misconduct Disclosure Scheme, Preamble

A template for the statement of conduct is available and requests information about the duration of employment, whether it has been proven that someone has committed misconduct, the nature of the misconduct, which disciplinary measures have been taken and any confirmation of ongoing investigation into allegations of misconduct. It should be noted that if the investigation is still in progress at the time of the application, the organisation will have a whistleblowing function and has to inform the other organisation if the investigation shows that misconduct was committed.

The Roadmap Screening as developed for the sector in The Netherlands is in line with and makes reference to the Misconduct Disclosure Scheme and will ensure standardisation of reference checks in terms of misconduct related information internationally. Similar to the Roadmap Screening, it allows organisations to share information about a person's integrity record through reference checks. While it makes sharing of integrity-related information more accessible, screening may take too long during an emergency response where staff needs to be deployed rapidly.

3.6 *INTERPOL pilot 'Operation Soteria'*

INTERPOL will pilot a project to improve global criminal records background checks for aid workers and provide advice to employers on international vetting and identification of high-risk individuals. The aim of this project is to stop perpetrators of abuse from working in the sector by improving global criminal records checks as well as information sharing between law enforcement agencies. This will be achieved by setting up a system through which employers can request criminal records data from around the world. The project will also have a capacity building programme whereby capacity is built in countries that do not have effective criminal record systems to strengthen criminal records checks and information sharing between INTERPOL members. The Advisory Board will include representatives from DFID, INTERPOL, ACRO Criminal Records Office, as well as Save the Children who will coordinate NGOs participating in the project.

The system is meant to give NGOs the ability to request background checks on candidates against national criminal records and INTERPOL criminal databases. In practice, this means that INTERPOL will facilitate requests from NGOs by requesting information from national law enforcement in respective countries, who will assess their data and share relevant information. As mentioned above, this system complements the Roadmap Screening in that requesting criminal background checks for candidates where a VOG cannot be issued should become easier. The system would nevertheless only include criminal data and not cover misconduct-related information that is not breaking national legislation.

3.7 *Digital ID System*

Save the Children in the United Kingdom (UK) has been working to develop a Digital ID System with three key functions: 1) provide someone with a unique ID; 2) provide a verified record of someone's employment history; and 3) provide organisations with information about previous grievances against someone regarding safeguarding concerns that have not been picked up by the police. The system is expected to address the issues of people getting into organisations that should not, and people moving between organisations that should not be re-hired. This ID system is most in line with what is generally understood to be a "humanitarian passport" whereby a candidate has a unique ID showing their employment history and integrity record during a recruitment process. It is meant to strengthen the overall integrity system and be used in parallel with other efforts, such as the Inter-Agency Misconduct Disclosure Scheme and INTERPOL project.

While originally the ID system was meant to be designed for the UK context at first, considering the breadth and ambition of the system, wider participation was sought. To encourage further engagement of the NGO sector but also to involve other governments, UN representation and law enforcement agencies, a Steering Committee has been proposed which would help guide the critical areas of this initiative including finding and utilising the right technology, ensuring accurate design requirements, overcoming legal and data protection concerns, etc. The proposal is for this alternative governance structure to be established will likely have significant leadership from DFID as well as sector experts in safeguarding, humanitarian recruitment and deployment, as well as technical experts in technology and information systems, employment and data protection law, monitoring and accountability. The establishment of the Steering Committee is yet to be determined, but it is anticipated that the work on this initiative will continue in 2019, including further development and testing of the system.

4. Conclusions and Recommendations

4.1 *Conclusions*

Many policies and procedures are already in place in the development and humanitarian sector to address integrity issues during the recruitment process as well as beyond the initial screening of new staff. However, reports on (sexually) transgressive behaviour and abuse of power in early 2018 showed there was a need for strengthening of these policies and procedures. In response, a Joint Integrity Action Plan was drafted by a broad coalition of non-governmental organisations to improve the prevention, signalling, enforcement and accountability of (sexually) transgressive behaviour and abuse of power in the sector. In order to streamline the screening process and ensure a uniform policy across the sector to screen new personnel which includes a stronger focus on integrity, a project team drafted the Roadmap Screening which briefly mentions a black list and “humanitarian passport” as instruments to share information related to integrity between organisations. This report presented the main findings on the feasibility of these instruments and also briefly explored other instruments being used or developed by other organisations or sectors.

There are a number of different instruments being used and developed across the sector and beyond to establish a system which prevents persons who have been convicted of (sexual) misconduct to enter into employment elsewhere in the sector. The Roadmap Screening is already set to be used since January 2019 and provide organisations with concrete tools to strengthen their screening on integrity issues. Instruments developed include the announcement text of the screening procedure, a self-declaration of good behaviour and application form, reference check template (including reference to the Misconduct Disclosure Scheme), Certificate of Conduct (VOG), and a checklist for recruiting integer staff.

The Roadmap Screening is expected to address – to an extent – the two key objectives of a potential integrity system (1 - identifying candidates with a previous record of (sexual) misconduct and/or abuse of power, and 2 - sharing of information so organisations can make an informed recruitment decision which includes misconduct related information). The main gaps not covered relate to the easy and quick access to information important for recruitment for quick deployments in case of emergencies, the lack of a whistleblowing function, and while information on integrity and misconduct is shared through reference checks, there is no central location where this kind of information is stored and accessible.

A persons register as used by the child care sector in The Netherlands was considered as one of the instruments that could address this gap. However, the register only contains information on the acceptance or rejection of someone's VOG and no other important information indicated by DRA members, such as disclosure of non-criminal integrity-related disciplinary action, references as well as a person's background and work experience. The required sector-specific legislation and regulations is also not available yet for the development and humanitarian sector and it is a costly system to develop. The VOG furthermore means it would be limited to The Netherlands thus limiting the information sharing between organisations internationally. A similar register for the development and humanitarian sector is thus not be the best instrument to increase information sharing on integrity issues.

Other instruments in use or under development internationally were also identified as potential instruments to address the identified gaps. This study looked into the UN Misconduct Tracking System (MTS), the Inter-Agency Misconduct Disclosure Scheme, the INTERPOL pilot project as well as the Digital ID system. The UN MTS is a system originally developed to track all allegations of misconduct from the point when it was received until the point when all required actions are taken which is now also used as a screening tool of new personnel, civilian and uniformed, deploying to UN field missions. Another vetting database is being developed by the Office of the Special Coordinator to be used across the UN System, but NGOs will not have access to this database for the time being.

The Inter-Agency Misconduct Disclosure Scheme has been developed as a minimum standard for sharing misconduct information as part of the recruitment process. At the time of introduction, misconduct was limited to sexual harassment, sexual abuse or sexual exploitation, but this may be broadened in time. The Roadmap Screening is in line with this Scheme and makes reference to it for international candidates, and while it is broader and provides more tools to improve screening in terms of misconduct, neither of them allows for quick screening needed during emergency deployments.

The INTERPOL pilot project to improve global criminal records background checks for aid workers will also complement the Roadmap Screening when it comes to international background checks. NGOs may request INTERPOL to facilitate this check with other countries. At the same time, INTERPOL will build capacity in several countries to strengthen their criminal record check systems. Developments around and results from the pilot project should be closely followed by organizations to advice on the applicability in The Netherlands.

The Digital ID System being developed in the UK is expected to provide registered persons a unique ID encompassing their employment records and grievances regarding safeguarding concerns. While it is closest to what is understood to be a "humanitarian passport", it is still meant to be implemented in complementarity with other instruments. At the time of writing, the establishment of a Steering Committee that draws in different NGOs, governments, UN agencies and law enforcement agencies is under consideration, and further development as well as testing and validation of the system are expected to take place in 2019. Before developing a similar system or implementing it in The Netherlands and other countries, these test results should be awaited.

Finally, a shared black list was explored as an option to address the identified gap. At the moment, some organisations use a black list internally and may reference it when providing professional references of (former) employees. The added value of a shared black list in addition to the Roadmap Screening instruments is the availability of misconduct registrations in one central place accessible to all organisations who have joined the shared black list. With a shared black list in place, participating

organisations can screen against previous misconduct records in a more pro-active manner, without depending on the references provided by a candidate. It does not however indemnify an organisation from conducting thorough screening as the black list information is only as accurate as the information provided by participating organisations.

A black list could be considered as a preferred instrument over a persons register because it is more in line with identifying candidates with a previous record of (sexual) misconduct and abuse, it also encompasses less personal data which makes it more concise, it has a lower administrative burden and it is easier to set up through the AP. There are also concerns which should be considered, including the need to find agreement among organisations about the protocol, which organisation/authority will be responsible for hosting and managing the black list, as well as carefully weighed and verifiable criteria for inclusion on the black list which takes into account protection and rights of beneficiaries and staff on the one hand and the rights of those whose (sexual) misconduct has been proven on the other hand. While a black list is only one of the instruments available to organisations to conduct as thorough a screening as possible, if agreement is found among organisations involved, it is likely to facilitate swift sharing of integrity-related information internationally once appropriate data protection measures are in place and authorisations obtained.

4.2 *Recommendations*

Based on the findings presented above, the following recommendations for the sector (led by branch organization(s)) are made:

1. **Suggest waiting for testing and validation results before developing a "humanitarian passport" similar to the Digital ID System under development in the UK.**

   The development of a "humanitarian passport" or similar system is expected to be complicated and rather than 're-inventing the wheel', it is recommended to wait for results of the testing of the ID system in the UK. Once the testing results are available, an assessment could be conducted to determine the added value of such a system or if it can easily be replicated or implemented in the Dutch context. In the meantime, the Roadmap Screening will provide a number of concrete tools to organisations to improve screening procedures related to integrity and if a sector-wide black list is pursued, more pro-active screening during recruitment will be enabled.

2. **Organisations should closely follow international developments, such as the INTERPOL pilot project and the Inter-Agency Misconduct Disclosure Scheme, and bring their processes in line with these.**

   No instrument covers all integrity screening aspects as part of the recruitment process and most complement each other, thus providing a more comprehensive picture of potential employees. It is therefore important to keep abreast of the development and implementation of other instruments.

Depending on how international initiatives progress, by the end of 2019 it may be worthwhile to consider the advantages of investing in a shared black list. The following considerations on this are recommended:

3. **Consider determining if a critical number of organisations would be interested to participate in a sector-wide black list and making available resources for the sector to further investigate the possibilities.**

   A consensus should exist among as many organisations as possible about the introduction of a sector-wide black list. In order for a black list to be shared within the sector in The Netherlands, a number of steps will furthermore need to be taken before a request for authorisation by the AP can be submitted. A DPIA will need to be conducted and, if this assessment shows a high privacy risk, the AP needs to be consulted prior to submitting a request for authorisation. Finally, a protocol describing how personal data will be processed and how this data processing complies with privacy legislation requirements needs to be developed. Sharing of the black list with participating organisations abroad will require additional steps which may require further authorisations, such as from European Data Protection Supervisors in the case of Binding Corporate Rules or the AP in the case of Standard Contractual Clauses with changes. These steps will require resources and legal expertise that need to be made available.

4. **Suggest identifying an organisation or authority who will be responsible for managing the shared black list in line with the GDPR.**

   If a black list is introduced in the sector, one organisation or authority should be responsible for its management and act as point of contact where participating organisations can request information from and provide inputs to.