DATA PROTECTION GUIDELINES

November 2015
FOREWORD

The key features of human trafficking, slavery and forced labour situations often involve a forced surrender of personal freedom, isolation, coercion, withdrawal of identity documents, abuse of vulnerabilities, restriction on freedom of movement and non-payment or withdrawal of wages. These means of exploitation and the devastating impact of different forms of exploitation are incredibly disempowering for the individual affected. Post-rescue, a victim’s long path to rehabilitation unwinds and is often complicated by interaction with law enforcement and the criminal justice system. The vulnerable individual is required by various actors to surrender and share personal details and accounts of exploitation. Victim support services require this data to better support survivors whilst law enforcement and other such actors are interested in data that can support the identification and prosecution of perpetrators.

In recognition of the value of survivor data to inform a better targeted response to the issue of modern day slavery, many efforts are currently ongoing to better harvest, record and analyse data. Given the great quest for better data and the interest of numerous stakeholders in obtaining data, it is more likely than not that essential data protection measures will unintentionally be overlooked. Somewhere along the lines the data becomes a statistic, a name and a number that is shared and disseminated, divorced from the vulnerable individual who owns the data. Misused sensitive information can lead to the identification of a very vulnerable individual who may be at risk of reprisals from a perpetrator. It is increasingly important that survivor data is treated and protected in accordance with the protections afforded by the law to ensure the proper checks and balances as prescribed by the law are used to protect vulnerable individuals.

Data protection is often an overlooked issue in organisations that are constantly firefighting and supporting very vulnerable people with very limited resources. We hope that these Guidelines will clarify the protections available in the law and assist NGOs with protecting sensitive data to better serve their clients and, ultimately, strengthen the fight against slavery.

Thank you to Reed Smith Richards Butler for their significant contribution to these Guidelines.

Archana Kotecha
Head of Legal
Liberty Asia
Whilst every effort has been made to ensure the accuracy of the information in this briefing note, this briefing note is not intended to constitute specific legal advice. We shall not bear any liability to any party in respect of the matters discussed herein.
Personal Data (Privacy) Ordinance (Cap. 486 of the Laws of Hong Kong)

A briefing note for NGOs working with victims of human trafficking

Information collected from victims in trafficking cases is valuable in assisting not only the victim but also potentially in assisting the identification of other potential and actual victims, trafficking networks and traffickers’ activities. This information is also essential for training professionals such as the police and immigration officers in handling human trafficking cases. At the same time, information received from victims of trafficking should be handled in a manner that protects the identity and interests of the victim. The purpose of this briefing note is to look at the basic legal principles of data privacy in the context of an NGO involved in advising or helping victims of potential human trafficking cases. These legal principles should be viewed as minimum requirements. NGOs should at all times handle personal data of victims with extra care and attention in view of the sensitive nature of the personal data involved, the likelihood of sharing personal data with law enforcement agencies and the possibility of transferring personal data overseas, the fragility of victims, and the risk to personal safety of the victims and potentially their family members in the event of leakage of personal data.

The Personal Data (Privacy) Ordinance (the "PDPO") was enacted in 1996. Its main objective is to protect the privacy rights of an individual in relation to his or her personal data. Any person who handles personal data in Hong Kong must comply with the six data protection principles (the "DPPs") set out in the PDPO.

DEFINITIONS

"Personal data"

"Personal data" is defined under the PDPO to mean any data relating (directly or indirectly) to a living individual from which it is practicable to identify such individual and which is in a form that can be accessed or processed. Almost all information an NGO collects from a victim beginning with the first interview falls within the wide definition of personal data.

Common examples of personal data include name, address, identity card number, passport number, phone number and other contact details of an individual. The definition under the PDPO is wide enough to include any information about an individual's behaviour, preferences or activities, which is stored with or can be cross-referenced to his or her identity. It can include both facts and opinions about such individual. Photographs or video footage of an identifiable individual may also constitute personal data.

"Data user"

A "data user" is a person (including legal entities) who, alone, jointly or in common with another person, controls the collection, holding, processing or use (including disclosure or transfer) of personal data, even if an aspect of the collection, holding, processing or use occurs outside of Hong Kong. NGOs which control the collection, holding, processing or use of
personal data are required to comply with the provisions of the PDPO, in particular, the six DPPs which are summarized below.

"Data subject"

A “data subject” is an individual who is the subject of the personal data. A “data subject” is also referred to in this briefing as a victim of trafficking.

THE SIX DPPS

The PDPO establishes six DPPs governing the collection, accuracy and duration of retention, use, security, and access to and correction of personal data. The DPPs also deal with information that should be made generally available. All data users must comply with these DPPs (subject to certain exceptions). The six DPPs are broadly summarized as follows:

DPP 1: Data collection principle

- Personal data must be collected for a lawful purpose directly related to a function or activity of the data user; the collection of the data must be necessary for or directly related to that purpose; and the data must be adequate but not excessive in relation to that purpose.
- Personal data must be collected by means, which are lawful and fair in the circumstances.
- All practicable steps must be taken to ensure that the data subject must be informed on or before collection of (a) whether it is obligatory or voluntary for him or her to supply the data (and the consequence of not so supplying the data); (b) the purpose (in general or specific terms) for which the data is to be used; (c) the classes of person to whom the data may be transferred; (d) the data subject’s right to request access to and correction of the data (on or before first use); and (e) the name or job title and address of the individual who is to handle data access and correction requests.

NGOs should consider providing victims with the information in the last bullet point in the form of a personal information collection statement ("PICS"). The PICS can for example be provided as part of or attached to a consent form or any form collecting personal information to be completed by the victim. Care should be taken to ensure that the PICS is reasonably prominent, easy to understand and easily legible. NGOs may also want to include certain relevant information from the PICS in a webpage, a telephone script or other notice.

In providing advice and helping a victim, questions will need to be asked about the victim, whether by way of an interview or on paper. The answers to such questions will frequently include personal data of the victim. Accordingly, carefully consider the necessity of collecting each item of information provided by the victim. In addition to considerations relating to collection of information, extreme care should be taken with regard to transferring personal data. Generally, personal data should be anonymized prior to transferring it outside of the NGO to ensure there is no way to link the information transferred to the identity of the victim.
Where it is necessary to transfer information that could be linked to the identity of the victim, policies and practices should be established to handle and limit the information transferred.

The victim’s interests must be weighed against the risks attached to the collection and transfer of the personal data. These risks include the abuse of data, corruption and information leaks (see DPP 4 below). Victims of trafficking risk retaliation from their traffickers and face significant challenges rebuilding their lives and re-integrating into society. The protection of a victim’s private life and identity is therefore essential for their physical safety. Further, victims who have been trafficked into forced criminal activities may be exposed to prosecution and social stigmatization if their personal data is leaked to authorities.

DPP 2: Accuracy and retention principle

- All practicable steps must be taken to ensure that any personal data held is accurate.
- Where there are grounds for believing that the personal data is inaccurate, the data should not be used unless and until those grounds cease to be applicable or the inaccurate data is erased.
- Where it is practicable to know that personal data disclosed to a third party is materially inaccurate, the third party must be informed that the data is inaccurate and provided with such particulars to enable the third party to rectify the data.
- All practicable steps must be taken to ensure that personal data is not kept longer than is necessary to fulfil the purpose for which it is intended to be used.
- If a data user engages a data processor (whether within or outside Hong Kong) to process personal data on its behalf, it must adopt contractual or other means to prevent any personal data transferred from being kept longer than is necessary for processing of the data.

It is advisable to have an internal policy or practice in place specifying the period of retention of personal data and what steps should be taken to erase personal data no longer required for the purpose for which the data was used.

DPP 3: Data use principle

- Personal data shall not be used for a new purpose without the prescribed consent of the data subject.
- Personal data must not be used for a new purpose even if consent has been given unless the data user has reasonable grounds for believing that the use of that data for the new purpose is clearly in the interest of the data subject.

When advising a victim, expressly explain the purpose of the collection of his or her personal data, including for potential criminal investigations and prosecution of third parties involved. The interest of the victim is of paramount importance in deciding how the personal data may be used, even if the victim has given his or her consent. Special attention should also be given to whether a victim is capable of giving real consent (i.e. valid consent), particularly in view of the vulnerability of a victim, his or her age and mental and physical condition. Every case will need
to be considered on its own merits, taking into account the particular circumstances of the victim.

**DPP 4: Data security principle**

- All practical steps must be taken to ensure that personal data is protected against unauthorised or accidental access, processing, erasure, loss or use having particular regard to:
  (a) The kind of data and the harm that could result if any of those things should occur;
  (b) The physical location where the data is stored;
  (c) Any security measures incorporated into any equipment in which the data is stored;
  (d) Any measures taken for ensuring the integrity, prudence and competence of persons having access to the data;
  (e) Any measures taken for ensuring the secure transmission of the data.
- If a data user engages a data processor (whether within or outside Hong Kong) to process personal data on behalf of the data user, the data user must adopt contractual or other means to prevent unauthorised or accidental access, processing, erasure, loss or use of the data transferred to the data processor for processing.

Given the sensitive nature of a victim’s personal data, personal data collected from a victim should be treated with extra care. It is strongly advisable to have in place a policy on, amongst other things, how personal data is to be treated and handled, the procedures for accessing personal data (including, where appropriate, limiting the number of NGO officers having access to the personal data to the case handlers only) and how personal data is to be kept secured. Personal data stored electronically in computers or portable storage devices should be protected with adequate IT security measures and access control.

Although the PDPO does not require notification of a security breach, notification is encouraged by the Privacy Commissioner for Personal Data (the "Commissioner").

**DPP 5: Openness principle**

- All practical steps must be taken to ensure that any person can ascertain the policies and practices of a data user in relation to personal data collected.
- All practical steps must be taken to ensure that any person can be informed of the kind of personal data held.
- All practical steps must be taken to ensure that any person can be informed of the main purposes for which the personal data are used.

NGOs should formulate privacy policy statements ("PPS"), stating the types of personal data held, the main purposes of use of each type of personal data and summarizing the privacy policies and practices in place. NGOs should make their PPS available including by displaying it on webpage and at reception counters.
In order to ensure full implementation of privacy policies and practices, trainings are crucial to ensure that NGO officers as well as volunteers and third party partners are aware of and will adhere to the stated policy and practice.

**DPP 6: Access to and correction principle**

- A data subject shall be entitled to ascertain whether a data user holds his or her personal data and request access to personal data.
- A data subject shall be entitled to be given reasons if a request of access to personal data is refused and object to a refusal.
- A data subject shall be entitled to request correction of personal data, be given reasons if a request for correction is refused and object to a refusal.¹

**TRANSFER OF PERSONAL DATA OUTSIDE OF HONG KONG**

There are restrictions in the PDPO on the transfer of personal data outside of Hong Kong but they have not yet come into force. At present, data users are required to comply with the general requirements of the PDPO when transferring personal data overseas, including DPP 3 stated above (i.e. the transfer must be for a purpose for which the data were to be used at the time of the collection of the data or a directly related purpose).

A clear expressed consent from a victim of trafficking is necessary to facilitate such transfer. In addition, given that such use and disclosure should be in the interest of the victim as embodied in DPP 3, it is important to ensure that personal data is only to be transferred for a purpose that is in the interest of the victim and to a jurisdiction where a similar data protection regime is in place to safeguard the security of such data. Finally, the data user should be aware that when transferring personal data to another jurisdiction, he or she may become subject to that jurisdiction’s data privacy laws, which may be more restrictive than the PDPO.²

**EXEMPTIONS**

There are a number of exemptions from compliance with the provisions of the PDPO (and hence from compliance with a particular DPP or all or most of the DPPs). Exemptions, which may apply to human trafficking cases, are exemptions to the restrictions on use and disclosure of personal data under DPP 3, where the use or disclosure of personal data is:

---
¹ Response to a data access request should be given within 40 days of receipt of the request. Otherwise, the data subject should be informed with reasons, and thereafter, full compliance with the request must be done as soon as practical.
² For example, in some countries, sensitive personal data of an individual’s ethnic or racial origin, political opinions, religious beliefs, physical or mental health condition, sexual life, commission or alleged commission of any offence, biometric data (such as DNA and fingerprint data) etc. requires additional protection as such information presents a greater risk to a person’s private life than “regular” person data. In Hong Kong, the PDPO does not differentiate personal data that are sensitive from those that are not and there are no specific provisions protecting sensitive personal data.
(a) required or authorised by any Hong Kong law or court order;

(b) required in connection with legal proceedings in Hong Kong or exercising or defending legal rights;

(c) for the purpose of preparing statistics or carrying out research (provided that no identifying information of any data subject is published).

REMEDIES FOR DATA SUBJECTS

NGOs should note that where there is a breach of the DPPs, a victim is entitled to make a complaint to the Commissioner. If the victim has suffered damage (including injury to feelings), he or she may also issue a civil action for compensation from the NGO.

Complaint to the Commissioner

Where a data user has contravened any requirement of the PDPO relating to an individual’s personal data, that individual or a relevant person of the individual may make a complaint to the Commissioner. The Commissioner will carry out an investigation to ascertain whether a contravention has occurred.

If the Commissioner determines that a contravention has occurred, the Commissioner may serve an enforcement notice directing the data user to remedy and (if appropriate) prevent any recurrence of the contravention. Failure to comply with the enforcement notice is a criminal offence, liable to a fine at level 5 (currently HK$50,000) and to imprisonment for two years, with a daily fine of HK$1,000 for a continuing offence. For a second and subsequent conviction for contravening an enforcement notice, the penalty is a fine at level 6 (currently HK$100,000) and imprisonment of two years, with a daily fine of HK$2,000 for a continuing offence.

Civil action for compensation against the data user

After the complaint has been concluded, the individual who has suffered damage (including injury to feelings) is entitled to seek compensation from the data user for that damage. The Commissioner may grant legal assistance (including legal advice and legal representation) to the aggrieved individual and the Commissioner will normally bear the costs of providing legal assistance.

RECOMMENDATIONS FOR NGOs

(a) Formulate a written and detailed data privacy policy that covers the handling of victim’s personal information from the first interview through to purging of the information.

---

3 Where the Commissioner decides not to serve an enforcement notice, the complainant (i.e. the data subject) may appeal to the Administrative Appeals Board against the Commissioner’s decision. Conversely, a data user may appeal to the Administrative Appeals Board against an enforcement notice not later than 14 days after it is served on him or her.
when no longer needed. The policy should cover amongst other things, what type of personal data should be collected, how personal data is to be treated and handled, the procedures for accessing personal data, and the requirements for anonymizing personal data prior to transferring to a third party.

(b) Develop a standardized Personal Information Collection Statement (PICS) and a consent form. Please refer to Appendix 1.

(c) Train all staff, volunteers and relevant third party partners on the NGO’s data privacy policy and on the use of the PICS and the consent form.

(d) Evaluate third parties (both public and private) to which the NGO might transfer personal data to determine if the third party has sufficiently robust policies, practices and systems to safeguard personal data.

(e) Ensure that the NGO’s IT systems are sufficiently secure and that access control measures are established.

(f) Formulate a privacy policy statement (PPS), which summarizes the NGO’s privacy policies and practices, and publication of the PPS (e.g. NGO’s website).

(g) Formulate a data retention policy that ensures that once personal data is no longer used for its intended purposes it will be purged.

(h) Appoint a designated NGO staff member to act as the NGO’s data privacy officer who will oversee implementation of the data policies and practices and training of staff, volunteers and relevant third party partners.
APPENDIX

Model of a Personal Information Collection Statement

PURPOSES OF COLLECTION

1. Personal data provided will be used by [name of NGO] for one or more of the following purposes:

(a) to assist you as a victim of human trafficking;

(b) to assist in identifying other potential or actual victims of human trafficking, trafficking networks and/or traffickers' activities on the condition your identity will be protected;

(c) for statistics and research purposes on the condition that the resulting statistics or results will not be made available in a form which will identify you;

(d) for training and educational purposes within the NGO; and

(e) any other legitimate purposes as may be required, authorised or permitted by law.

2. Fields marked with an asterisk (*) on the form attached are mandatory. If you fail to provide the required data, we may not be able to assist you.

CLASSES OF TRANSFEREES

3. We will not disclose personal data collected from you to any other party without your prior consent, save where it is required, authorised or permitted by law. [NB: If personal data may be transferred, state the types of organisations or classes of persons to whom the personal data may be transferred. Identify the transferees where possible. Note that transferees cannot be described in a general form.]

RETENTION OF DATA

4. We will keep your personal data only for as long as necessary to fulfil the purpose(s) for which the data was collected. We may also retain archived personal data for statistical purposes.

5. Personal data, which is no longer required, will be destroyed.
SECURITY

6. Except as mentioned above, your personal data, however stored, will be accessed only by our staff members or volunteers who are authorised to do so. Where personal data is stored electronically, it will be password-protected (or under some equivalent form of protection) and accessible only by authorised personnel. Staff members or volunteers designated to handle personal data will be instructed to do so for the abovementioned purpose(s) for which personal data are to be used.

7. [Insert any security measures adopted in the handling of personal data.]

8. ACCESS TO AND CORRECTION OF PERSONAL DATA

9. You have a right, at any time, to request access to and correction of your personal data in any of our records. To exercise any of your rights, contact us at the address, facsimile number or email stated below, marking your communication "Confidential”. In response, we may ask you to provide certain details about yourself so that we can be sure that you are the person to whom the data refers. We will respond to your request within 40 days after receiving it.

10. Enquiries concerning the personal data collected by means of the form attached, including requesting access to and correction of your personal data, should be addressed to:

   Personal Data Privacy Officer (Attention: [insert name])
   [name of NGO]
   [address]
   Facsimile number: [insert number]
   Email address: [insert email address]