Ujvala Consultants Private Limited
#37, Ujvala, 20th Main
BSK First Stage, Bangalore 560050
Web: www.ujvala.com:E mail: naavi@naavi.org: Mob: 9343554943

P.S: This draft was being prepared as part of the PDPSI code of practice. It will still undergo changes. However, the untimely death of Mr Neeraj Arora, advocate and Cyber Evidence expert in Delhi has prompted me to place this as a draft policy under CLCC and dedicate it to his memory.

Naavi

Draft Code of Practice

And

Draft Policy for handling Personal data of Deceased Data Principals

Objective

The objective of this Policy is to establish a method for handling the personal data of an individual who is known to be or is suspected to be deceased.

Background:

An organization would be in possession of personal data of an individual collected with appropriate informed consent.

The Consent is a "Contract" with an offer document in the form of a Privacy Notice" by the Data fiduciary and an acceptance by the Data Principal through an affirmative opt-in. In certain cases, the offer is in the nature of "Invitation to offer" which is accepted by the Data Fiduciary.

The offer and acceptance documents are authenticated to make them admissible in a Court of law either by the use of a valid digital/electronic signature or through a certified form of electronic document (eg: Certificate under Section 65B of Indian Evidence Act in India).

Alternatively, the offer and acceptance need to be authenticated with the collection and retention of such meta data that would be acceptable in a court of law as reasonable evidence of the free consent having been obtained.

When personal information is collected directly from the data principal in consideration of any service offered, the consent is recorded before the processing of the personal data and conforms to the requirements of a comprehensive notice which highlights the principles of processing, the rights of the data principal including the right of withdrawal of the consent, the form of grievance redressal etc. This contains the disclosure of the purpose of collection, details of the type of information collected, the retention period, cross border transfer if any, transfer to other co-data fiduciaries or data processors etc. as covered by the basic "Purpose Specific Privacy Policy" of the organization.

When a data principal expires, the status of the data principal and the compliance obligations change. In some data protection regulations, the applicability of the compliance obligations may continue for a period after the death of the data principal (Eg: Singapore law where the definition of a natural person extends to deceased persons and the obligations of personal data protection extends to 10 years after death).

When the lawful basis for collection and processing of personal data is “Consent”, the death of a person (as well as loss of contractual capacity such as insanity or insolvency) immediately terminates the contract. Hence the “Consent” no longer remains valid. Additionally if the law is meant to protect the privacy right of a living natural person, the applicability of the law also ceases.

Any instruction of a natural person regarding disposal of the information after his/her death is a testamentary document (like a Will) and in some laws (eg Indian Information Technology Act 2000), an electronic document which is testamentary in nature is not recognized in law.

Hence the consent obtained before the death of a data principal will be invalid on the receipt of the notice of death by the Data Fiduciary. The personal data collected under such invalidated consent no longer has the status of the protected personal data as per the subject data protection law.

Such information is also not in the form of “Anonymized” personal information since it may still contain the individually identifiable parameters and hence cannot be considered equivalent to “Non Personal Information”.

Since most of the data protection laws are not clear about how to deal with such “Personal data of Deceased Data Principal” (PD-DDP), this addendum policy is created as an extension of the Purpose specific Privacy Policy and covers the identification, continued use, archival, deletion etc of the personal data of deceased data principals including “Suspected deceased data principals”.

Policy

Discovery of PD-DDP

1. The organization makes a reasonable effort to scan the public information available in cyber space to identify if there is any knowledge about the death of an individual whose personal data may be available in their repository.

   A search of publicly available obituary data or data which may indicate the possible instances of death of data principals whose personal data is in the custody of the organizations is conducted at regular intervals (not exceeding one month) to identify potential sets of personal data of deceased persons in the repository of personal data in the custody of the organization.

   Such identified information is classified and flagged as “PD-RDDP”. (Personal Data of reportedly deceased data principal).

2. The organization under its “Purpose Specific Privacy Policy” (PSPP) sends a personal data confirmation request once every year to the last known e-mail of the data principal requesting confirmation of the current version of the PSPP. In the event no reply is received within 7 days of the receipt of such a notice or if the email bounces for reasons such as “No Such account exists”, the consent confirmation is escalated to the next level of confirmation where a reminder is sent through another mode of communication if available (eg: SMS through mobile). If no response is received for this message within 2 days, the request for consent is

escalated to the third level where a notice is sent to the individual in at least two modes of communication that the account will be placed under suspension unless the confirmation is received within 24 hours.

3. In the event no response is received, the case is referred by the DPO to the Data Governance Committee recommending transfer of the personal data to a "Dormant-Suspected deceased status". The continued use of such data will depend on existence of any legitimate interest of the organization including the need to account for any financial transactions between the organization and the individual. Such data would be transferred to a secondary data storage space and would be subject to a higher level of security.
4. Where there is no legitimate interest in continuing the processing of the data, dormant data would be archived in an encrypted state and not processed further in the normal course. Any subsequent request for access shall be treated as an "Incident" and resolved with appropriate verification and authentication by the DPO.
5. Where the personal data remains dormant for more than 2 years, the data shall be further tagged as "Inoperative-Strongly Suspected deceased" status and moved to a tertiary archive of such data which is encrypted. Any subsequent request for access shall be treated as an "Incident" and resolved with appropriate verification and authentication by the DPO.
6. Where the personal data remains in-operative for more than 5 years, the "Consent prohibiting disclosure" is considered as in-operative and a notice shall be published in a Cyber notice service such as "Cyber-Notice.com". After a further period of one month, if no claim for the information comes from either the data principal or any legal representative, a notice is sent to the Data Protection Authority or any other designated authority that the data may be transferred to their custody for further archival. In the event the authority refuses to receive such data, the data may be deleted or anonymized and converted into Non Personal data.
7. Any time after an account is flagged "Dormant", the Data Fiduciary shall endeavour to identify the legal heirs of the suspected deceased data principal and initiate a claim process from their end.
8. Where the data fiduciary has a data asset of the data principal in his custody and money is being received as royalty or otherwise and an attempt to make payments to the data principal fails because the transaction bounces or the receiving banker refuses to collect the amount for any reason (even without confirming the death of the account holder), the accumulated asset and money is considered as held in trust for the Data Fiduciary and his legal heirs. The money in such accounts shall be kept in the form of a special reserve of "Unclaimed Balances" with the data fiduciary.
9. Where the data fiduciary receives a confirmation of death, the information is verified through appropriate means and the known legal heirs are notified directly and through Cyber notification to file their claim for settlement as per procedure outlined below. Pending settlement of the claim a new tag of "Under Claim Settlement Process" is assigned to the data set and shall be moved into a data vault with appropriate security in terms of encryption and access control. When the claim is settled, the information is released to the successful claimant after holding a copy thereof for contingent requirement for a further period of 180 days after which it may be deleted.
10. After a personal data is classified as "Inoperative" and appropriate public notice through Cyber Notice system is served for which no response is received, it is considered that the data fiduciary assumes a legitimate interest to process the information as per this policy.
11. In order to facilitate the claim process in case of death, every account holder is provided with an option to nominate an "Alternate" e-mail ID or a designated nominee who would be

considered as a virtual representative for the purpose of managing the account after the death of the data principal.

12. For Indian data principals, an option would be provided to the individual to deposit the instructions on how to handle the account after death of the data principal through a letter in writing since “electronic Will” is not recognized in India. The physical letter would be considered as the original instruction and the e-mail will be an electronic copy. The physical letter would be archived without opening and only when the report of the death of the deceased person is received, it would be opened to confirm the electronic instruction.

Claim Settlement Process

1. A legal heir of a deceased data principal may approach a data fiduciary on knowing that the deceased data principal had an account with the data fiduciary such as an E Mail account or a Drop Box account etc where some valuable personal data or data which belonged to the deceased person (including non personal data) may be present.
2. He/she would not be having the password to the account and even if he had the password, it would be incorrect for him to log in in the name of the deceased since it would amount to impersonation under law.
3. Further the property of a deceased person may belong to several legal heirs and unless the deceased has nominated an individual to receive the property for the purpose of re-distribution.
4. The legal heirs would be required to file a joint claim declaring themselves to the only surviving heirs of the deceased who died intestate as to the said digital property. The letter signed by all shall be supported by an eKYC based on Aadhaar or by a Bank Manager or a Court order.
5. The Claim process would be charged a nominal fee of Rs 1000/- or such other fee that the Data Protection Authority may determine as a reimbursement of expenses.
6. On receipt of a valid claim, the Data Protection Committee shall approve the disclosure of the information to the claimant/s and archive the data for a period of further 180 days as a contingent back up.
7. After the expiry of the 180 days cooling time, the data may be destroyed.
8. In the event the data has already been transferred to the Data Protection authority the claim may be diverted to the appropriate authority for further action.

Any dispute arising out of this policy shall be resolved with online mediation and/or arbitration through DDMAC. (Data Disputes Mediation and Arbitration Center of FDPPI) or through the Adjudicator under the personal Data protection act.