**Annex 1**

**Part 1 - Relevant Legislations and Interpretation of the Laws**

1. **Constitution**

**9. Protection for privacy of home and other property**

(1) Except with his own consent, no person shall be subjected to the search of his person or his property or the entry by others on his premises.

(2) Nothing contained in or done under the authority of any law shall be held to be inconsistent with or in contravention of this section to the extent that the law in question makes provision—

(a) in the interests of defence, public safety, public order, public morality, public health, town and country planning, the development or utilisation of mineral resources or the development or utilisation of any other property in such a manner as to promote the public benefit;

(b) for the purpose of protecting the rights or freedoms of other persons;

(c) to enable an officer or agent of the Government or a local authority, or a body corporate established by law for a public purpose, to enter on the premises of any person in order to value those premises for the purpose of any tax, rate or due, or in order to carry out work connected with any property that is lawfully on those premises and that belongs to the Government, the local authority or that body corporate, as the case may be; or

(d) to authorise, for the purpose of enforcing the judgment or order of a Court in any civil proceedings, the search of any person or property by order of a Court or the entry upon any premises by such order;

except so far as that provision or, as the case may be, the thing done under its authority is shown not to be reasonably justifiable in a democratic society.

**16. Protection from discrimination**

(1) Subject to subsections (4), (5) and (7), no law shall make any provision that is discriminatory either of itself or in its effect.

(2) Subject to subsections (6), (7) and (8), no person shall be treated in a discriminatory manner by any person acting in the performance of any public function conferred by any law or otherwise in the performance of the functions of any public office or any public authority.

(3) In this section, “discriminatory” means affording different treatment to different persons attributable wholly or mainly to their respective descriptions by race, caste, place of origin, political opinions, colour, creed or sex whereby persons of one such description are subjected to disabilities or restrictions to which persons of another such description are not made subject or are accorded privileges or advantages that are not accorded to persons of another such description.

(4) Subsection (1) shall not apply to any law so far as that law makes provision—

(a) for the appropriation of revenues or other funds of Mauritius;

(aa) for a minimum number of candidates for election to local authorities to be of a particular sex, with a view to ensuring adequate representation of each sex on a local authority;

[Inserted 35/11 (cio 1212/11).]

(ab) for a minimum number of candidates for election to the Rodrigues Regional Assembly to be of a particular sex, with a view to ensuring adequate representation of each sex in the Rodrigues Regional Assembly;

[Inserted 30/16 (cio 17/12/16).]

(b) with respect to persons who are not citizens of Mauritius; or

(c) for the application, in the case of persons of any such description as is mentioned in subsection (3) (or of persons connected with such persons), of the law with respect to adoption, marriage, divorce, burial, devolution of property on death or other like matters that is the personal law applicable to persons of that description.

(5) Nothing contained in any law shall be held to be inconsistent with or in contravention of subsection (1) to the extent that it makes provision with respect to standards or qualifications (not being standards or qualifications specifically relating to race, caste, place of origin, political opinions, colour, creed or sex) to be required of any person who is appointed to any office in the public service, any office in a disciplined force, any office in the service of a local authority or any office in a body corporate established directly by any law for public purposes.

(6) Subsection (2) shall not apply to anything which is expressly or by necessary implication authorised to be done by any such provision of law as is referred to in subsection (4) or (5).

(7) Nothing contained in or done under the authority of any law shall be held to be inconsistent with or in contravention of this section to the extent that the law in question makes provision whereby persons of any such description as is mentioned in subsection (3) may be subjected to any restriction on the rights and freedoms guaranteed by sections 9, 11, 12, 13, 14 and 15, being such a restriction as is authorised by section 9 (2), 11 (5), 12 (2), 13 (2), 14 (2) or 15 (3), as the case may be.

(8) Subsection (2) shall not affect any discretion relating to the institution, conduct or discontinuance of civil or criminal proceedings in any Court that is vested in any person by or under this Constitution or any other law.

1. **Data Protection Act 2017**

Under the DPA, the general principle

Relevant sections of the DPA for an organisation developing / using AI solutions include:

|  |  |
| --- | --- |
| **Section** | **Interpretations/ Provisions of the law(*in italics*)** |
| **2 – Interpretation** | Personal data is defined as “*any information relating to a data subject*”.  A controller is defined as “*a person who or public body which, alone or jointly with others, determines the purposes and means of the processing of personal data and has decision making power with respect to the processing*” whereas a processor is “*a person who, or public body which, processes personal data on behalf of a controller”.* |
| **3 – Application of the Act** | The Data Protection Act (DPA) 2017 applies to “*the processing of personal data, wholly or partly, by automated means and to any processing otherwise than by automated means where the personal data form part of a filing system or are intended to form part of a filing system”* Section 3(3)  The Data Protection Act applies to a controller or processor who -   1. *is established in Mauritius and processes personal data in the context of that establishment; and* 2. *is not established in Mauritius bus uses equipment in Mauritius for processing personal data, other than for the purpose of transit through Mauritius.*   Section 3(5) |
| **4 – Establishment of Office** | Under Section 4, the Data Protection Office, which is the enforcing body, is established and is as follows:  *(1) There shall, for the purposes of this Act, be a public office to be known as the Data Protection Office.*  *(2) In the discharge of its functions under this Act, the Office shall act with complete independence and impartiality and shall not be subject to the control or direction of any other person or authority.*  *(3) The head of the Office, who shall be known as the Data Protection Commissioner, shall be a barrister of not less than 5 years’ standing.*  *(4) The Commissioner shall be assisted by such public officers as may be necessary.*  *(5) Every public officer referred to in subsection(4) shall be under the administrative control of the Commissioner.* |
| **5 – Functions of Commissioner** | The Head of the Office is the Data Protection Commissioner whose functions,include the following –   1. ***ensure compliance with this Act and any regulations made under it;*** 2. *issue or approve such Codes of Practice or Guidelines for the purposes of theis Act as he thinks fit;* 3. *maintain a register of controllers and processors;* 4. ***exercise control on all data processing operations, either of his own motion or at the request of a data subject, and verify whether the processing of data is done in accordance with this Act;*** 5. *promote self-regulation among controllers and processors;* 6. ***investigate any complaints or information which gives rise to a suspicion that an offence may have been, is being or is about to be, committed under this Act;*** 7. *take such measures as may be necessary to bring the provisions of this Act to the knowledge of the general public;* 8. ***undertake research into, and monitor developments in, data processing, and ensure that there is no significant risk or adverse effect of any development s on the privacy of individuals****;* 9. ***examine any proposal for automated decision making or data linkage that may involve an interference with, or may otherwise have an adverse effect, on the privacy of individuals and ensure that any adverse effect of the proposal on the privacy of individuals is minimized;*** 10. *coorperate with necessary authorities of other countries, to the extent necessary for the performance of his duties under the Act, in particular by exchanging relevant information in accordance with any other enactment; and* 11. *do anyrhing incidental or conducive to the attainment of the objects of and to the better performance of his duties and functions under, this Act.*   The Data Protection Commissioner will exercise control on all data processing operations, either of his own motion or at the request of a data subject, and verify whether the processing of data is done in accordance with the Act. |
| **14 – Controller and Processor** | An organisation using or developing AI solutions must register as a controller or processor with the Data Protection Office. |
| **21 – Principles relating to processing of personal data** | 1. Lawfulness, Fairness and Transparency *-* Personal data shall be *processed lawfully, fairly and in a transparent manner in relation to any data subject.* 2. Purpose Limitation - Personal data shall be *collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.* 3. Data Minimisation - Personal data shall be adequate, relevant and not excessive in relation to the purpose. 4. Accuracy *- Personal data shall be accurate and where necessary kept up to date, with every reasonable step being taken to ensure that any inaccurate personal data are erased or rectified without delay;* 5. Storage Limitation - Personal data shall be *kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.* 6. Rights of Data Subjects - Personal shall be *processed in accordance with the rights of data subjects.* |
| **23 - Collection of personal data** | Under the DPA, the general principle is that the consent of an individual is required before the sharing of personal data can be done and that individual must under Section 23 of the DPA, be informed of that at the time of collection of the personal data.  A controller must not collect personal data unless –  *(a) it is done for a lawful purpose connected with a function or activity of the controller; and*  *(b) the collection of the data is necessary for that purpose.*  Provides details to the data subject as per section 23 (2)   * + The organisation’s contact details and where applicable its representative and any data protection officer;   + Purpose(s) for which you are collecting the data;   + To whom you intend to disclose the data;   + Whether the collection is voluntary or mandatory;   + Right to withdraw consent at any time;   + Rights of data subjects: Access, Rectification, Erasure, Object to Processing;   + Automated decision making, and the consequences of such processing;   + Period for storing the data;   + Right to lodge a complaint with the Commissioner;   + To which countries they intend to transfer the data, |
| **28 – Lawful processing** | Section 28 lays down the conditions for lawful processing to take place.  There are **9 available lawful basis for processing:**   1. Consent or 2. (i) for the performance of a contract; or   (ii) for compliance with any legal obligation;  (iii) to protect vital interests of the data subject;  (iv) for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;  (v) for the performance of any task carried out by a public authority;  (vi) for the exercise, by any person in the public interest, of any other functions of a public nature;  (vii) for the legitimate interests pursued by the controller except if the processing is unwarranted in any particular case having regard to the harm and prejudice to the rights and freedoms or legitimate interests of the data subject;  (viii) for the purpose of historical, statistical or scientific research. |
| **29 – Special Categories of personal data** | If the AI solutions is or will be procession special categories of personal data. The controller will need to satisfy a condition under section 28 and any condition of section 29 (1) such as   * The processing carried out in course of legitimate activities by a foundation, association or not for profit body; * The processing relates to personal data which are manifestly made public by the data subject; * The processing is necessary for * Establishment, exercise or defence of a legal claim; or * Purpose of preventive or occupational medicine, assessment of the working capacity of an employee, medical diagnosis, the provision of health or social care; or * Purpose carrying out the obligations and exercising specific rights of the controller or the data subjects; or * Protecting the vital interests of the data subject |
| **31 – Security of Processing** | Appropriate technical and organisational measures must be implemented to prevent unauthorised access to, alteration, disclosure, accidental loss and destruction of personal data.  Such measures include:   * Pseudonymisation and encryption of personal data * Ensure ongoing confidentiality, integrity, availability, and resilience of processing systems * Ability to restore availability and access to personal data in a timely manner in the event of a physical or technical incident * Process for regularly testing, assessing, and evaluating the effectiveness of technical organizational measures   If the controller is using the services of a processor, the controller is still responsible under the DPA for data protection and must ensure through a written contract that the processor acts only on instructions received from the controller and implements appropriate security measures for protecting any personal data processed. |
| **32 – Prior security check** | *(1) Where the Commissioner is of the opinion that the processing or transfer of data by a controller or processor may entail a specific risk to the privacy rights of data subjects, he may inspect and assess the security measures taken under section 31 prior to the beginning of the processing or transfer.*  *(2) The Commissioner may, at any reasonable time during working hours, carry out further inspection and assessment of the security measures imposed on a controller or processor under section 31.* |
| **34 – Data Protection Impact Assessments** | A DPIA is mandatory when the processing is likely to result in a high risk for the rights and freedom of individuals, including some specified types of processing such as:   * Use systematic and extensive profiling or automated decision-making to make significant decisions about people * Process special category data on a large scale. * Systematically monitor a publicly accessible place on a large scale.   A DPIA is recommended for the implementation of AI solutions. |
| **37 to 41- Rights of data subjects** | 1. Right of access – Section 37   A data subject has the right to obtain confirmation that his/her personal data is processed and a copy of the data free of charge within one month following a written request.   1. Automated individual decision making – Section 38  * A data subject has the right not to be subject to a measure which is based on profiling by means of automated processing. * Can be carried out by the controller if it is necessary for a contract, authorised by law or based on the explicit consent of the data subject.  1. Rectification –Section 39  * A data subject has the right to obtain from controller rectification of inaccurate or incomplete personal data concerning him/her.  1. Erasure – Section 39  * A data subject may request that his/her personal data are erased if the continued processing of those data is not justified.  1. Restriction of Processing – Section 39  * A data subject may request that the processing of his/her personal data is restricted where the accuracy of the data is contested.  1. Object – Section 40  * A data subject has the right to object in writing at any time the processing of personal data relating to him/her free of charge.  1. Exercise of rights – Section 41  * Any right conferred on an individual in this Act may be exercised * where the data subject is a minor, by a person who has parental authority over the minor or has been appointed as his guardian; * where the data subject is physically or mentally unfit, by a person who has been appointed as his guardian or legal administrator by a Court; or * in any other case, by a person duly authorised in writing by the data subject to make a request. |
| **46 – Compliance audit** | The Commissioner is empowered to carry out periodical audits of information systems and security systems used by the controllers and processors. |

The Data Protection Act can be accessed on the following link:

<https://mitci.govmu.org/Documents/Legislations/The%20Data%20Protection%20Act%202017.pdf>

1. **Computer Misuse and Cybercrime Act 2003**

The Act provides for the repression of criminal activities perpetrated by using computer systems and criminalises unauthorized access to computer date (Section 3) and access with intent to commit offences (Section 4). The enforcing body is the Police CyberCrime Unit.

Relevant Sections include:

**3. Unauthorised access to computer data**

(1) Subject to subsections (2) and (3), any person who causes a computer system to perform a function, knowing that the access he intends to secure is unauthorised, shall commit an offence and shall, on conviction, be liable to a fine not exceeding 50,000 rupees and to penal servitude for a term not exceeding 5 years.

(2) A person shall not be liable under subsection (1) where—

(a) he is a person with a right to control the operation or use of the computer system and exercises such right in good faith;

(b) he has the express or implied consent of the person, empowered to authorise him, to have such an access;

(c) he has reasonable grounds to believe that he had such consent as specified in paragraph (b);

(d) he is acting pursuant to measures that can be taken under Part III of this Act; or

(e) he is acting in reliance of any statutory power arising under any enactment for the purpose of obtaining information, or of taking possession of, any document or other property.

(3) An access by a person to a computer system shall be unauthorised where the person—

(a) is not himself entitled to control access of the kind in question; and

(b) does not have consent to access by him of the kind in question from any person who is so entitled.

(4) For the purposes of this section, it is immaterial that the unauthorised access is not directed at—

(a) any particular program or data;

(b) a program or data of any kind; or

(c) a program or data held in any particular computer system.

**4. Access with intent to commit offences**

(1) Any person who causes a computer system to perform any function for the purpose of securing access to any program or data held in any computer system with intent to commit an offence under any other enactment, shall commit an offence and shall, on conviction, be liable to a fine not exceeding 200,000 rupees and to penal servitude for a term not exceeding 20 years.

(2) For the purposes of this section, it is immaterial that—

(a) the access referred to in subsection (1) is authorised or unauthorised;

(b) the further offence to which this section applies is committed at the same time when the access is secured or at any other time.

PART III – INVESTIGATIONS AND PROCEDURES

**11. Preservation order**

(1) Any investigatory authority may apply to the Judge in Chambers for an order for the expeditious preservation of data that has been stored or processed by means of a computer system or any other information and communication technologies, where there are reasonable grounds to believe that such data is vulnerable to loss or modification.

(2) For the purposes of subsection (1), data includes traffic data and subscriber information.

(3) An order made under subsection (1) shall remain in force—

(a) until such time as may reasonably be required for the investigation of an offence;

(b) where prosecution is instituted, until the final determination of the case; or

(c) until such time as the Judge in Chambers deems fit.

**12. Disclosure of preserved data**

The investigatory authority may, for the purposes of a criminal investigation or the prosecution of an offence, apply to the Judge in Chambers for an order for the disclosure of—

(a) all preserved data, irrespective of whether one or more service providers were involved in the transmission of such data;

(b) sufficient data to identify the service providers and the path through which the data was transmitted; or

(c) electronic key enabling access to or the interpretation of data.

**13. Production order**

(1) Where the disclosure of data is required for the purposes of a criminal investigation or the prosecution of an offence, an investigatory authority may apply to the Judge in Chambers for an order compelling—

(a) any person to submit specified data in that person’s possession or control, which is stored in a computer system; and

(b) any service provider offering its services to submit subscriber information in relation to such services in that service provider’s possession or control.

(2) Where any material to which an investigation relates consists of data stored in a computer, disc, cassette, or on microfilm, or preserved by any mechanical or electronic device, the request shall be deemed to require the person to produce or give access to it in a form in which it can be taken away and in which it is visible and legible.

**14. Powers of access, search and seizure for purposes of investigation**

(1) Where an investigatory authority has reasonable grounds to believe that stored data would be relevant for the purposes of an investigation or the prosecution of an offence, it may apply to a Judge in Chambers for the issue of a warrant to enter any premises to access, search and seize such data.

(2) In the execution of a warrant under subsection (1), the powers of the investigatory authority shall include the power to—

(a) seize or secure a computer system or any information and communication technologies medium;

(b) make and retain a copy of such data or information;

(c) maintain the integrity of the relevant stored data or information; or

(d) render inaccessible or remove the stored data or information from the computer system, or any information and communication technologies medium.

**15. Real time collection of traffic data**

Where the investigatory authority has reasonable grounds to believe that any data would be relevant for the purposes of investigation and prosecution of an offence under this Act, it may apply to the Judge in Chambers for an order—

(a) allowing the collection or recording of traffic data, in real time, associated

with specified communications transmitted by means of any computer system; or

(b) compelling a service provider, within its technical capabilities, to—

(i) effect such collection and recording referred to in paragraph (a); or

(ii) assist the investigatory authority to effect such collection and recording.

**16. Deletion order**

A Judge in Chambers may, upon application by an investigatory authority, and being satisfied that a computer system or any other information and communication technologies medium contains an indecent photograph of a child, order that such data be—

(a) no longer stored on and made available through the computer system or any other medium; or

(b) deleted or destroyed.

1. **Code Civile Mauricien**

**Article 22 – Du respect de la vie privée**

*Chacun a droit au respect de sa vie privée.*

*Les jurisdictions compétentes peuvent, sans préjudice de la réparation du dommage subi, prescrire toute mesures, tells que séquestre, saisie et autres, propre à empêcher ou faire cesser une atteinte à l’intimité de la vie privée.*

*Ces mesures peuvent, s’il y a urgence, être ordonnées par le Juge en Chambre.*

Interpretation: By virtue of the above, any individual who considers that his rights to a private life is being infringed may seek legal redress, including the urgent intervention of the Judge in Chambers.

1. **Prevention of Terrorism Act 2002**

Sections 25 (1) and (4) and 25A provides that the interception of information and digital materials and the use of electronic and technical devices for the purpose of intelligence gathering or surveillance are specifically allowed.

Provisions of the Law:

**25. Intelligence gathering**

(1) Notwithstanding any other enactment, the Minister may, for the purpose of the prevention or detection of offences, or the prosecutions of offenders, under the Act, give such directions as may be necessary to –

(a) communication service providers generally;

(b) communication service providers of a specified description;

(c) any particular communication service provider –

(i) not to disclose any data or data of any description;

(ii) to retain any data subjects to such requirements or restrictions as he may determine.

(4) In this section:

“communication service provider” means a person who provides a postal, or an information and communication, including telecommunications, services:

“data” means information recorded in a form in which it can be processed by equipment operating

automatically in response to instruction given for that purpose.

**25A. Special powers of enquiry**

(1) Notwithstanding any other enactment, where the Commissioner has reasonable ground to believe that an offence under this Act has been, is being or is likely to be committed by any person, he may apply to a Judge in Chambers for an order authorising a police officer not below the rank of Superintendent to use such electronic and technical device as may be required for the purpose of intelligence gathering or surveillance.

(2) Where, on an application under subsection (1), the Judge in Chambers is satisfied that the Commissioner has reasonable ground to suspect that an offence has been, is being or is likely to be committed, the Judge may grant the order.

1. **The DNA Idenfitication Act 2009**

Section 9 (2) of the DNA Identification Act provides that a DNA sample shall be destroyed by the Forensic Science Laboratory (FSL) as soon as it has fulfilled the purpose for which it was taken or after the final determination of any proceedings in relation to which the sample was taken.

Relevant provision:

**9. Taking, storage, preservation and destriuuction of DNA Sample**

(1) Every DNA sample shall be taken by a qualified person and stored and preserved in accordance with such procedure and guidelines as may be laid down by the FSL.

(2) Subject to subsection (3) and (4) and section 10(5), a DNA sample shall be destroyed by the FSL as soon as it has fulfilled the purpose for which it was taken or after the final disposal of any proceedings in relation to which the sample was taken, whichever occurs later.

(3) (a) Subject to paragraph (b), a DNA sample may be kept for such reasonable time as may be appropriate for the purpose of research or the constitution of its DNA Data Records of DNA Population Statistical Database.

(b) No research shall be undertaken pursuant to paragraph (a) without the approval of the Minister.

(4) A Court may, where it is satisfied that a DNA sample may reasonably be required in an investigation or a prosecution of a person for an offence, order that the DNA sample shall not be destroyed during such period as the Court considers appropriate.

(5) Notwithstanding the preceding subsections, a DNA sample collected at a scene of crime may be kept for as long as the Commissioner of Police or the FSL deems it desirable to do so unless the destruction of the sample is ordered by the Court.

**10. DNA Data Records**

(5) Where a person has consented to give his DNA sample under this Act, that consent may be reoved by giving written notice to the Director and the Direction shal cause the DNA sample to be destroyed and the resulting profile be erased from the DNA Data Records within a period of one year from the date of receipt of the revocation.

1. **The Electronic Transactions Act 2000**

The Electronic Transactions Act is relevant only as regards to protecting privacy in digital communications. Its enforcing body is the ICTA and the Act provides the legal framework to facilitate electronic transactions and communications by regulating electronic signatures and the security thereof.

1. **The Civil Aviation Regulations 2007**

Regulation 91C (1) (d) and (e) provides that a remotely piloted aircraft or a remotely piloted surveillance aircraft weighing not more than 7 kilogrammes, which is flown strictly for leisure or recreational purposes, should not be flown over the property of any person unless the permission of that person has been obtained, and over any area to which the public has access.

Relevant Regulation:

**Regulation 91C. Remotely piloted aircraft or remotely piloted surveillance aircraft used for leisure or recreational purposes**

(1) Regulations 91 and 91A shall not apply to a remotely piloted aircraft or a remotely piloted surveillance aircraft weighing not more than 7 kilogrammes, which is flown strictly for leisure or recreational purposes, provided that the aircraft is not flown –

(a) in Class A airspace, Class C airspace, Class D airspace or Class E airspace without the permission of the Authority;

(b) within an aerodrome traffic zone during the notified hours of watch of the air traffic control unit at that aerodrome unless permission of the air traffic control unit is obtained;

(c) at a height exceeding 400 feet above the surface unless it is flying in airspace specified in subparagraph (a) or (b) and in accordance with the requirements for that airspace;

(d) over the property of any person unless the permission of that person has been obtained;

(e) over any area to which the public has access; or

(f) at night.

(2) No person shall fly, for leisure or recreational purposes, a remotely piloted aircraft or a remotely piloted surveillance aircraft which weighs more than 7 kilogrammes but less than 20 kilogrammes without its fuel, but including any article or equipment installed in or attached to the aircraft at the commencement of its flight.

(3) Where a person intends to fly, for leisure or recreational purposes, a remotely piloted aircraft or a remotely piloted surveillance aircraft in an airspace specified in paragraph 1(a) or in a zone and at a time specified in paragraph 1(b), he shall make an application seeking the permission of the Authority in such manner as the Authority may determine.

(4) Where the applicant meets the conditions set out in the civil airworthiness requirements specified in regulation 135 for flying a remotely piloted aircraft or a remotely piloted surveillance aircraft weighing not more than 7 kilogrammes for leisure or recreational purposes, the Authority shall, on payment of the appropriate fee specified in the Sixteenth Schedule, grant permission to the applicant.

1. **The Information and Communication Technologies Act 2001**

The enforcing body is the Information and Communication Technologies Authority (ICTA).

The Act can be accessed on the following link:

<https://mitci.govmu.org/Documents/Legislations/ICT%20Act%202001%20Amended.pdf>

**Part 2 – Additional Information**

**1. Mobile App - ‘Lespwar’**

On 25th November 2020, a mobile app ‘Lespwar’ was launched by the government in collaboration with the Ministry of Gender Equality and Family Welfare on the occasion of the International Day for the Elimination of Violence against Women and the UNDP.

The mobile app is a tool to alert the police and the authorities for assistance by simply pressing the ‘Panic Button’ on the mobile app for cases of Gender Based Violence (GBV). The Service Requestor will have to download the application on his/her smart phone via Google Play Store, free of charge. Prior to the registration, the user will have to agree with the terms and conditions. The app only collects location data during user registration and when ‘Send help’ button is pressed. It does not collect location data in the background. Once the panic button is pressed, the Police Main Command and Control Centre (PMCCC) will receive a notification in the backend. In case the user has no internet connection and presses the panic button, the alert will be diverted to a toll free SMS and will be sent to the PMCCC. The PMCCC will trace out the victim by the integrated GPS system in the mobile app and inform the Police officer nearest to the place of incident. Requests as far as practicable will be attended within 15 minutes.

The Police will provide assistance to the victims as well as collateral victims who are in need of medical attention. They will also record declaration and statements, and arrest the perpetrators where applicable. Officers from the Police Family Protection unit will remain on call on a daily basis to attend to cases of domestic violence and will ensure follow-up of the cases at their respective unit. For cases where the victims request for psychological support or shelter, the Ministry of Gender Equality and Family Welfare will be contacted for support. Other related features on the Mobile app are support networks, information on the Protection from Domestic Violence Act (PDVA).