MANE CHANCE SANCTUARY

Data Protection (GDPR) Policy

1. Introduction.

Background

1.1 Mane Chance Sanctuary (MCS) needs to collect person-identifiable information about individuals in order to carry out its functions and fulfil its objectives. Personal data is defined as 'information which relates to a living individual and from which they can be identified, either directly or indirectly'.
1.2 Personal data at MCS can include Trustees, employees (present, past and prospective), volunteers, contractors and third parties, supporters, donors, private and confidential information as well as sensitive information, whether in paper, electronic or other form.
1.3 Irrespective of how information is collected, recorded and processed person identifiable information must be dealt with properly to ensure compliance with the Data Protection Act (DPA) 1998 and the forthcoming General Data Protection Regulations (GDPR).
1.4 The DPA requires MCS to comply with the eight Data Protection Principles (see Appendix A below).
1.5 The DPA gives rights to data subjects (people that we hold information about) to access their own personal information, to have it corrected if wrong, in certain permitted circumstances to ask us to stop using it and to seek damages where we are using it improperly.
1.6 The lawful and correct treatment of person-identifiable information by MCS is paramount to the success of the organisation and to maintaining the confidence of its employees and supporters. This policy will help MCS ensure that all person-identifiable information is handled and processed lawfully and correctly.

Data Protection Act and GDPR principles

1.7 MCS has a legal obligation to comply with all relevant legislation in respect of data protection and information / IT security.
1.8 All legislation relevant to an individual's right to the confidentiality of their information and the ways in which that can be achieved and maintained are paramount to MCS. Significant penalties can be imposed upon the organisation or its employees for non-compliance.
1.9 The aim of this policy is to outline how MCS meets its legal obligations in safeguarding confidentiality and adheres to information security standards. The obligations within this policy are principally based upon the requirements of the Data Protection Act 1998 and the forthcoming GDPR, as the key legislative and regulatory provisions governing the security of person-identifiable information.

2. What information is covered?

2.1 Personal data within the respective legislative and regulatory provisions covers 'any data that can be used to identify a living individual either directly or indirectly'. Individuals can be identified by various means including but not limited to, their address, telephone number or e-mail address. Anonymised or aggregated data is not regulated by the provisions, providing the anonymisation or aggregation of the data is irreversible.
2.2 Sensitive personal data is referred to in the GDPR as 'special categories of personal data', which are broadly the same as those in the Data Protection Act (DPA) 1998. These specifically include the processing of genetic data, biometric data and data concerning health matters.

3. Policy statement.

3.1 This document defines the data protection policy for MCS. It applies to all person-identifiable information obtained and processed by the organisation and its employees. It sets out:

- the organisation's policy for the protection of all person-identifiable information that is processed;
- establishes the responsibilities (and best practice) for data protection;
- references the key principles of the Data Protection Act 1998 and GDPR.

4. Principles.

4.1 In accordance with the requirements outlined in the GDPR, personal data will be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals.
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- Accurate and, where necessary, kept up-to-date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

- 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; personal data may be stored for longer periods, insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

4.2 The GDPR also require that 'the controller shall be responsible for, and able to demonstrate, compliance with the principles.'

5. Accountability.

5.1 Mane Chance Sanctuary will implement appropriate technical and organisational measures to demonstrate that data is processed in line with the principles set out in the GDPR.

5.2 Records of activities relating to higher risk processing will be maintained, such as the processing of special categories data or that in relation to criminal convictions and offences.

5.3 Internal records of processing activities will include the following:

- Name and details of the organisation
- Purpose(s) of the processing
- Description of the categories of individuals and personal data
- Retention schedules
- Categories of recipients of personal data
- Description of technical and organisational security measures
- Details of transfers to third countries, including documentation of the transfer mechanism safeguards in place

5.4 MCS will implement measures that meet the principles of data protection by design and data protection by default, such as:

- Data minimisation.
- Use of pseudonyms where appropriate.
- Transparency.
- Allowing individuals to monitor processing.
- Continuously creating and improving security features.

5.5 Data protection impact assessments will be used, where appropriate.

6. Policy.

6.1 MCS obtains and processes person-identifiable information for a variety of different purposes, including but not limited to:

- staff records and administrative records;
- volunteer records;
- donor records;
- supporter records including event attendance;
- complaints and requests for information.

6.2 Such information may be kept in either computer or manual records. In processing such personal data MCS will comply with the data protection principles within the Data Protection Act 1998.

7. Data protection responsibilities.

Overall responsibilities.

7.1 MCS Board members, collectively known as the 'data controller' permit the organisation's personnel to use computers and relevant filing systems (manual records) in connection with their duties. MCS Board members have legal responsibility for the compliance of the Data Protection Act 1998.
7.2 MCS Board members, whilst retaining their legal responsibilities, have delegated data protection compliance to the Data Protection Officer. The individual appointed as DPO will have professional experience and knowledge of data protection law, particularly that in relation to charities.

Data Protection Officer's (DPO) responsibilities.

7.3 The Data Protection Officer's responsibilities include:

- Ensuring that the policy is produced and kept up to date.
- Ensuring that the appropriate practice and procedures are adopted and followed by MCS.
- Provide advice and support to the Board on data protection issues within the organisation.
- Work collaboratively with the General Manager to help set the standard of data protection training for MCS personnel.
- Endure compliance with individual rights, including subject access requests.
- Act as a central point of contact on data protection issues within the Charity.
- Implement an effective framework for the management of data protection.

Line Managers' responsibilities.

7.4 All line managers across the organisation's business units are directly responsible for:

- ensuring their staff are made aware of this policy and any notices.
- ensuring their staff are aware of their data protection responsibilities.
- ensuring their staff receive suitable data protection training.

General responsibilities.

7.5 All MCS personnel, including administrative volunteers, are subject to compliance with this policy. Under the GDPR individuals can be held personally liable for data protection breaches.

7.6 All MCS personnel have a responsibility to inform the Data Protection Officer of any new use of personal data, as soon as reasonably practicable after it has been identified.

7.7 All MCS personnel will, on receipt of a request from an individual for information held, known as a subject access request or concerns about the processing of personal information, immediately notify the Data Protection Officer.

7.8 MCS employees must follow the subject access request procedure (see section 11 below).

8. Lawful processing.

8.1 The legal basis for processing data will be identified and documented prior to data being processed. Under the GDPR, data will be lawfully processed under the following conditions:

- The consent of the data subject has been obtained.
- Processing is necessary for:
    - Compliance with a legal obligation.
    - The performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
    - For the performance of a contract with the data subject or to take steps to enter into a contract.
    - Protecting the vital interests of a data subject or another person.
    - For the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject.

8.2 Sensitive data will only be processed under the following conditions:

- Explicit consent of the data subject, unless reliance on consent is prohibited by EU or Member State law.
- Processing carried out by a not-for-profit body with a political, philosophical,

religious or trade union aim provided the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without consent.

- Processing relates to personal data manifestly made public by the data subject.
- Processing is necessary for:
  - Carrying out obligations under employment, social security or social protection law, or a collective agreement.
  - Protecting the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent.
  - The establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity.
  - Reasons of substantial public interest on the basis of Union or Member State law which is proportionate to the aim pursued and which contains appropriate safeguards.
  - The purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of Union or Member State law or a contract with a health professional.
  - Reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices.
  - Archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article 89(1).

9. Consent.

9.1 Consent must be a positive indication. It cannot be inferred from silence, inactivity or pre-ticked boxes.

9.2 Consent will only be accepted where it is freely given, specific, informed and an unambiguous indication of the individual's wishes.

9.3 Where consent is given, a record will be kept documenting how and when consent was given.

9.4 MCS ensures that consent mechanisms meet the standards of GDPR. Where the standard of consent cannot be met, an alternative legal basis for processing the data must be found, or the processing must cease.

9.5 Consent accepted under the DPA will be reviewed to ensure that it meets the standards of the GDPR; however, acceptable consent obtained under the DPA will not be re-obtained.

9.6 Consent can be withdrawn by the individual at any time.

9.7 The consent of parents will be sought prior to the processing of a child's data, except where the processing is related to preventative or counselling services offered directly to a child.

10. The right to be informed.

10.1 The privacy notice supplied to individuals in regards to the processing of their personal data will be written in clear, plain language which is concise, transparent, easily accessible and free of charge.
10.2 If services are offered directly to a child, the trust will ensure that the privacy notice is written in a clear, plain manner that the child will understand.
10.3 In relation to data obtained both directly from the data subject and not obtained directly from the data subject, the following information will be supplied within the privacy notice:

- The identity and contact details of the DPO.
- The purpose of, and the legal basis for, processing the data.
- The legitimate interests of the controller of the third party.
- Any recipient or categories of recipients of the personal data.
- The retention period of criteria used to determine the retention period.
- The existence of the data subject's rights, including the right to:
    - Withdraw consent at any time.
    - Lodge a complaint with a supervisory authority.
- The existence of automated decision making, including profiling, how decisions are made, the significance of the process and the consequences.

10.4 Where data is obtained directly from the data subject, information regarding whether the provision of personal data is part of a statutory or contractual requirement and the details of the categories of personal data, as well as any possible consequences of failing to provide the personal data, will be provided.
10.5 Where data is not obtained directly from the data subject, information regarding the source of the personal data originates from and whether it came from publicly accessible sources, will be provided,
10.6 For data obtained directly from the data subject, this information will be supplied at the time the data is obtained.
10.7 In relation to data that is not obtained directly from the data subject, this information will be supplied:

- Within one month of having obtained the data.
- If disclosure to another recipient is envisaged, at the latest, before the data are disclosed.
- If the data are used to communicate with the individual, at the latest,

when the first communication takes place.

11. The right of access.

11.1 Individuals have the right to obtain confirmation that their data is being processed.
11.2 Individuals have the right to submit a subject access request (SAR) to gain access to their personal data in order to verify the lawfulness of the processing.
11.3 MCS will verify the identity of the person making the request before any information is supplied.
11.4 A copy of the information will be supplied to the individual free of charge; however, MCS may impose a 'reasonable fee' to comply with requests for further copies of the same information.
11.5 Where a SAR has been made electronically, the information will be provided in a commonly used electronic format.
11.6 Where a request is manifestly unfounded, excessive or repetitive, a reasonable fee will be charged.
11.7 All fees will be based on the administrative cost of providing the information.
11.8 All requests will be responded to without delay and at the latest, within one month of receipt.
11.9 In the event of numerous or complex requests, the period of compliance will be extended by a further two months. The individual will be informed of this extension, and will receive an explanation of why the extension is necessary, within one month of the receipt of the request.
11.10 Where a request is manifestly unfounded or excessive, MCS holds the right to refuse to respond to the request. The individual will be informed of this decision and the reasoning behind it, as well as their right to complain to the supervisory authority and to a judicial remedy, within one month of the refusal.
11.11 In the event that a large quantity of information is being processed about an individual, MCS will ask the individual to specify the information the request is in relation to.

12. The right to rectification.

12.1 Individuals are entitled to have any inaccurate or incomplete personal data rectified.
12.2 Where the personal data in question has been disclosed to third parties, MCS will inform them of the rectification where possible.
12.3 Where appropriate, MCS will inform the individual about the third parties that the data has been disclosed to.
12.4 Requests for rectification will be responded to within one month; this will be extended by two months where the request for rectification is complex.
12.5 Where no action is being taken in response to a request for rectification, MCS will explain the reason for this to the individual, and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

13. The right to erasure.

13.1 Individuals hold the right to request the deletion or removal of personal data where there is no compelling reason for its continued processing.
13.2 Individuals have the right to erasure in the following circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed;
- When the individual withdraws their consent;
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing;
- The personal data was unlawfully processed;
- The personal data is required to be erased in order to comply with a legal obligation;
- The personal data is processed in relation to the offer of information society services to a child.

13.3 MCS has the right to refuse a request for erasure where the personal data is being processed for the following reasons:

- To exercise the right of freedom of expression and information;
- To comply with a legal obligation for the performance of a public interest task or exercise of official authority;
- For public health purposes in the public interest;
- For archiving purposes in the public interest, scientific research, historical research or statistical purposes;
- The exercise or defence of legal claims.

13.4 As a child may not fully understand the risks involved in the processing of data when consent is obtained, special attention will be given to existing situations where a child has given consent to processing and they later request erasure of the data, regardless of age at the time of the request.

13.5 Where personal data has been disclosed to third parties, they will be informed about the erasure of the personal data, unless it is impossible or involves disproportionate effort to do so.
13.6 Where personal data has been made public within an online environment, MCS will inform other organisations who process the personal data to erase links to and copies of the personal data in question.

14. The right to restrict processing.

14.1 Individuals have the right to block or suppress the MCS's processing of personal data.
14.2 In the event that processing is restricted, MCS will store the personal data, but not further process it, guaranteeing that just enough information about the individual has been retained to ensure that the restriction is respected in future.
14.3 MCS will restrict the processing of personal data in the following circumstances:

- Where an individual contests the accuracy of the personal data, processing will be restricted until MCS has verified the accuracy of the data;
- Where an individual has objected to the processing and MCS is considering whether their legitimate grounds override those of the individual;
- Where processing is unlawful and the individual opposes erasure and requests restriction instead;
- Where MCS no longer needs the personal data but the individual requires the data to establish, exercise or defend a legal claim .

14.4 If the personal data in question has been disclosed to third parties, MCS will inform them about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so.
14.5 MCS will inform individuals when a restriction on processing has been lifted.

15. The right to data portability.

15.1 Individuals have the right to obtain and reuse their personal data for their own purposes across different services.
15.2 Personal data can be easily moved, copied or transferred from one IT environment to another in a safe and secure manner, without hindrance to usability.
15.3 The right to data portability only applies in the following cases:

- To personal data that an individual has provided to a controller;
- Where the processing is based on the individual's consent or for the performance of a contract;
- When processing is carried out by automated means.

15.4 Personal data will be provided in a structured, commonly used and machine-readable form.

15.5 MCS will provide the information free of charge.
15.6 Where feasible, data will be transmitted directly to another organisation at the request of the individual.
15.7 MCS is not required to adopt or maintain processing systems which are technically compatible with other organisations.
15.8 In the event that the personal data concerns more than one individual, MCS will consider whether providing the information would prejudice the rights of any other individual.
15.9 MCS will respond to any requests for portability within one month.
15.10 Where the request is complex, or a number of requests have been received, the timeframe can be extended by two months, ensuring that the individual is informed of the extension and the reasoning behind it within one month of the receipt of the request.
15.11 Where no action is being taken in response to a request, MCS will, without delay and at the latest within one month, explain to the individual the reason for this and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

16. The right to object

16.1 MCS will inform individuals of their right to object at the first point of communication, and this information will be outlined in the privacy notice and explicitly brought to the attention of the data subject, ensuring that it is presented clearly and separately from any other information.
16.2 Individuals have the right to object to the following:

- Processing based on legitimate interests or the performance of a task in the public interest.
- Direct marketing.
- Processing for purposes of scientific or historical research and statistics.

16.3 Where personal data is processed for the performance of a legal task or legitimate interests:

- An individual's grounds for objecting must relate to his or her particular situation.
- MCS will stop processing the individual's personal data unless the processing is for the establishment, exercise or defence of legal claims, or, where the trust can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual.

16.4 Where personal data is processed for direct marketing purposes:

- MCS will stop processing personal data for direct marketing purposes as soon as an objection is received.
- MCS cannot refuse an individual's objection regarding data that is being processed for direct marketing purposes.

16.5 Where personal data is processed for research purposes:

- The individual must have grounds relating to their particular situation in order to exercise their right to object.
- Where the processing of personal data is necessary for the performance of a public interest task, MCS is not required to comply with an objection to the processing of the data.

16.6 Where the processing activity is outlined above, but is carried out online, MCS will offer a method for individuals to object online.

17. Privacy by design and privacy impact assessments.

17.1 MCS will act in accordance with the GDPR by adopting a 'privacy by design' approach and implementing technical and organisational measures which demonstrate how the trust has considered and integrated data protection into processing activities.
17.2 Data protection impact assessments (DPIAs) will be used to identify the most effective method of complying with MCS's data protection obligations and meeting individuals' expectations of privacy.
17.3 DPIAs will allow MCS to identify and resolve problems at an early stage, thus reducing associated costs and preventing damage from being caused to the Charity's reputation which might otherwise occur.
17.4 A DPIA will be used when using new technologies or when the processing is likely to result in a high risk to the rights and freedoms of individuals.
17.5 A DPIA will be used for more than one project, where necessary.
17.6 High risk processing includes, but is not limited to, the following:

- Systematic and extensive processing activities, such as profiling;
- Large scale processing of special categories of data or personal data which is in relation to criminal convictions or offences.

17.7 MCS will ensure that all DPIAs include the following information:

- A description of the processing operations and the purposes;
- An assessment of the necessity and proportionality of the processing in relation to the purpose;
- An outline of the risks to individuals;
- The measures implemented in order to address risk.

17.8 Where a DPIA indicates high risk data processing, MCS will consult the ICO to seek its opinion as to whether the processing operation complies with the GDPR.

18. Data breaches.

18.1 The term 'personal data breach' refers to a breach of security which has led to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.
18.2 The DPO will ensure that all staff members are made aware of, and understand, what constitutes as a data breach as part of their continuous development training.
18.3 Where a breach is likely to result in a risk to the rights and freedoms of individuals, the relevant supervisory authority will be informed.
18.4 All notifiable breaches will be reported to the relevant supervisory authority within 72 hours of MCS becoming aware of it.
18.5 The risk of the breach having a detrimental effect on the individual, and the need to notify the relevant supervisory authority, will be assessed on a case-by-case basis.
18.6 In the event that a breach is likely to result in a high risk to the rights and freedoms of an individual, MCS will notify those concerned directly.
18.7 A 'high risk' breach means that the threshold for notifying the individual is higher than that for notifying the relevant supervisory authority.
18.8 In the event that a breach is sufficiently serious, the public will be notified without undue delay.
18.9 Effective and robust breach detection, investigation and internal reporting procedures are in place at MCS, which facilitate decision-making in relation to whether the relevant supervisory authority or the public need to be notified.
18.10 Within a breach notification, the following information will be outlined:

- The nature of the personal data breach, including the categories and approximate number of individuals and records concerned;
- The name and contact details of the DPO;
- An explanation of the likely consequences of the personal data breach;
- A description of the proposed measures to be taken to deal with the personal data breach;
- Where appropriate, a description of the measures taken to mitigate any possible adverse effects.

18.11 Failure to report a breach when required to do so will result in a fine, as well as a fine for the breach itself.

19. Data security.

19.1 Confidential paper records will be kept in a locked filing cabinet, drawer or safe, with restricted access.
19.2 Confidential paper records will not be left unattended or in clear view anywhere with general access.
19.3 Digital data is coded, encrypted or password-protected, both on a local hard drive and on a network drive that is regularly backed up off-site.

19.4 Where data is saved on removable storage or a portable device, the device will be kept in a locked filing cabinet, drawer or safe when not in use.
19.5 Memory sticks will not be used to hold personal information unless they are password-protected and fully encrypted.
19.6 All electronic devices are password-protected to protect the information on the device in case of theft.
19.7 Emails containing sensitive or confidential information are password-protected if there are unsecure servers between the sender and the recipient.
19.8 Circular emails to supporters are sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients.
19.9 When sending confidential information by fax, staff will always check that the recipient is correct before sending.
19.10 Where personal information that could be considered private or confidential is taken off the premises, either in electronic or paper format, staff will take extra care to follow the same procedures for security, e.g. keeping devices under lock and key. The person taking the information from MCS premises accepts full responsibility for the security of the data.
19.11 Before sharing data, all staff members will ensure:

- They are allowed to share it.
- That adequate security is in place to protect it.
- Who will receive the data has been outlined in a privacy notice.

19.12 Under no circumstances are visitors allowed access to confidential or personal information. Visitors to areas of MCS containing sensitive information are supervised at all times.
19.13 The physical security of MCS's buildings and storage systems, and access to them, is reviewed on a regular basis. If an increased risk in vandalism/burglary/theft is identified, extra measures to secure data storage will be put in place.
19.14 Mane Chance Sanctuary takes its duties under the GDPR seriously and any unauthorised disclosure may result in disciplinary action.
19.15 The Data Protection Officer is responsible for continuity and recovery measures are in place to ensure the security of protected data.

20. Publication of information.

20.1 Some classes of information are made routinely available, including:

- Annual Reports;
- Financial information;
- Policies and procedures.

20.2 Mane Chance Sanctuary will not publish any personal information, including photos, on its website without the permission of the affected individual.
20.3 When uploading information to the MCS website, staff are considerate of any metadata or deletions which could be accessed in documents and images on the site.

21. Photography.

21.1 MCS will always indicate its intentions for taking photographs of staff and visitors and will retrieve permission before publishing them.
21.2 If MCS wishes to use images/video footage of visitors in a publication, such as the MCS website or social media sites, written permission will be sought for the particular usage.
21.3 Images captured by individuals for recreational/personal purposes, and videos made by visitors for family use, are exempt from the GDPR.

22. Data retention.

22.1 Data will not be kept for longer than is necessary.
22.2 Unrequired data will be deleted as soon as practicable.
22.3 Paper documents will be shredded, and electronic memories scrubbed clean or destroyed, once the data should no longer be retained.

23. DBS data.

23.1 All data provided by the DBS will be handled in line with data protection legislation; this includes electronic communication.
23.2 Any third parties who access DBS information will be made aware of the data protection legislation, as well as their responsibilities as a data handler.

24. Monitoring.

24.1 Compliance with this policy will be monitored by the Risk and Finance Sub-Committee.
24.2 The Data Protection Officer is responsible for the monitoring, revision and updating of this policy document on an annual basis or sooner, should the need arise.

25. Validity of this policy.

25.1 This policy will be reviewed annually by the MCS Board. Associated data protection standards will be subject to an ongoing development and review programme.

26. Legal framework.

26.1 This policy has due regard to legislation, including, but not limited to the following:

- The General Data Protection Regulation (GDPR) 2018
- The Data Protection Act 1998
- The Freedom of Information Act 2000

26.2 This policy will also have regard to the following guidance:

- Information Commissioner's Office (2017) 'Overview of the General Data Protection Regulation (GDPR)'.
- Information Commissioner's Office (2017) 'Preparing for the General Data Protection Regulation (GDPR) 12 steps to take now'.

Appendix A.
Data Protection Act 1998 – data protection principles.

1. Personal data shall be processed fairly and lawfully.

2. Personal data shall be obtained for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

4. Personal data shall be accurate and, where necessary, kept up to date.

5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purpose.

6. Personal data shall be processed in accordance with the rights of data subjects under this Act.

7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.