Zambia

Data Protection Act, 2021

Act 3 of 2021

Legislation as at 24 March 2021

FRBR URI: /akn/zm/act/2021/3/eng@2021-03-24

There may have been updates since this file was created.

PDF created on 21 February 2024 at 18:41.

Collection last checked for updates: 31 December 1996.

Check for updates

About this collection

The legislation in this collection has been reproduced as it was originally printed in the Government Gazette, with improved formatting and with minor typographical errors corrected. All amendments have been applied directly to the text and annotated. A scan of the original gazette of each piece of legislation (including amendments) is available for reference.

Data Protection Act, 2021
Contents

Part I – Preliminary 1
1. Short title and commencement 1
2. Interpretation 1
3. Application 4
Part II – Office of the Data Protection Commissioner 4
4. Establishment of Office of Data Protection Commissioner 4
5. Data Protection Commissioner 4
6. Appointment of Deputy Data Protection Commissioners and other staff 5
Part III – Inspectorate 5
7. Inspector 5
8. Power of inspectors 5
9. Arrest without warrant 6
10. Seizure of property 6
11. Restoration of property 6
Part IV – Principles and rules relating to processing of personal data 7
12. Principles relating to processing of personal data 7
13. Processing of personal data 7
14. Processing of sensitive personal data 7
15. Consent, justification and objection 8
16. Collection of personal data 8
17. Processing of child and vulnerable person's personal data 9
18. Offence and penalty for contravention of personal data obligation 9
Part V – Regulation of data controllers, data processors and data auditors 9
19. Prohibition from controlling or processing personal data without registration 9
20. Application for registration as data processor or data controller 10
21. Registration of data controller and data processor 10
22. Renewal of certificate of registration 10
23. Change in details of data controller or data processor 10
24. Suspension or cancellation of registration 10
25. Re-registration 11
26. Surrender of certificate of registration 11
27. Exemption from registration 11
28. Power to forbear 11
Part VI – Data auditors 12

29. Data auditors 12
30. Application for licence 12
31. Issue of licences 12
32. Conditions of licence 12
33. Variation of licence 12
34. Surrender of licence 13
35. Transfer or licence 13
36. Suspension and cancellation 13
37. Renewal of licence 14
38. Functions of data auditor 14
Part VII – Exemptions from principles and rules of processing of data 15
39. National security, defence and public order 15
40. Prevention, detection, investigation and prosecution of contraventions of law 15
41. Processing for purposes of legal proceedings 15
42. Research, archiving or statistical purposes 15
43. Journalistic purpose 15
44. Processing to be lawful and legitimate 16
Part VIII – Duties of data controller and data processor 16
45. Record of processing activities 16
46. Data protection impact assessment 16
47. Security of processing 16
48. Appointment of data protection officer 17
49. Notification of security breach 17
50. Accountability 17
51. Data retention 17
52. Duties of data processor 18
53. Non-disclosure of personal data 18
54. Joint controllers 18
55. Offence by data controller 19
56. Personal data in legal proceedings 19
57. Notification 19
Part IX – Rights of the data subject 19
58. Right of access and notification 19
59. Right to rectification 20
60. Right to erasure 20

61. Right of objection 20
62. Decision taken on basis of automatic data processing 21
63. Right to restriction of processing 21
64. Information when personal data collected directly from data subject 22
65. Right to data portability 22
66. Notification obligation 22
67. Derogation from rights 22
68. Complaints 23
69. Appeals 23
Part X – Transfer of personal data outside the Republic 23
70. Cross-border transfer of personal data 23
71. Conditions for cross-border transfer of personal data 23
Part XI – General provisions 24
72. Right to compensation 24
73. Offences 24
74. Power of Data Protection Commissioner to compound certain offences 24
75. Forfeiture 24
76. Offence by principal officer shareholder or partner of body corporate or unincorporate body 24
77. General penalty 25
78. Code of conduct 25
79. Guidelines 25
80. Register 25
81. Auditing of data controller 26
82. Regulations 26

Zambia

Data Protection Act, 2021

Act 3 of 2021

Published in Government Gazette on 24 March 2021

Assented to on 23 March 2021

Commenced on 1 April 2021 by Data Protection Act (Commencement) Order, 2021

[This is the version of this document from 24 March 2021.]

An Act to provide an effective system for the use and protection of personal data; regulate the collection, use, transmission, storage and otherwise processing of personal data; establish the Office of the Data Protection Commissioner and provide for its functions; the registration of data controllers and licencing of data auditors; provide for the duties of data controllers and data processors; provide for the rights of data subjects; and provide for matters connected with, or incidental to, the foregoing.

ENACTED by the Parliament of Zambia.

Part I – Preliminary

1. Short title and commencement

This Act may be cited as the Data Protection Act, 2021, and shall come into operation on the date appointed by the Minister by statutory instrument.

2. Interpretation

In this Act, unless the context otherwise requires—

"**anonymisation**" means the process of removing direct and indirect personal identifiers that may lead to an individual being identified;

"**Authority**" means the Zambia Information Communications and Technology Authority established by the Information Communications and Technologies Act, 2009;

[Act No. 15 of 2009]

"**automated**" in relation to data, means electronically transmitted in whole or in part, by means of a data message in which the conduct of a data message of one or more parties are not reviewed by a natural person in the operation of the electronic system, in the ordinary course of that natural person's business or employment;

"**biometric data**" means Personal data resulting from scientific analysis relating to the physical, physiological or behavioural characteristics of a natural person, which confirm the unique identification of that natural person;

"**child**" has the meaning assigned to the word in the Constitution;

[Cap. 1]

"**child abuse**" includes physical and emotional neglect, physical injury, other than accidental injury, ill treatment and sexual abuse of a child;

"**child abuse data**" means personal data consisting of information as to whether the child data subject is or has been the subject of, or may be at risk of, child abuse;

"**code of conduct**" means a data protection charter approved by the Authority which regulates the conduct of a data controller or data processor, in order to ensure that the data controller or data processor of personal data complies with this Act and any other applicable written law;

"**Commission**" means the Competition and Consumer Protection Commission established by the Competition and Consumer Protection Act, 2010;

[Act No. 24 of 2010]

"**consent**" means any written, freely given, specific, informed and unambiguous indication of the data subject's wishes by which such data subject, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to that data subject;

"**consumer**" has the meaning assigned to the word in the Competition and Consumer Protection Act, 2010;

[Act No. 24 of 2010]

"**data**" means numbers, letters, alphabetic or numeric strings, symbols or codes in any form;

"**data auditor**" means a person licensed as a data auditor under section 29;

"**data controller**" means a person who, either alone or jointly with other persons, controls and is responsible for keeping and using personal data on a computer, or in structured manual files, and requests, collects, collates, processes or stores personal data from or in respect of a data subject;

"**data processor**" means a person, or a private or public body that processes personal data for and on behalf of and under the instruction of a data controller;

"**Data Protection Commissioner**" means a person appointed as Data Protection Commissioner under section 5;

"**data retention**" means a process of retention of personal data for a specified purpose for a defined period;

"**data subject**" means an individual from, or in respect of whom, personal information is processed;

"**genetic data**" means any personal information relating to the inherited or acquired genetic characteristics of an individual which result from the analysis of a biological sample from the individual in question, in particular chromosomal deoxyribonucleic acid (DNA) or ribonucleic acid (RNA) analysis, or from the analysis of another element enabling equivalent information to be obtained;

"**health practitioner**" has the meaning assigned to the word under the Health Professions Act, 2009;

[Act No. 24 of 2009]

"**Independent Broadcasting Authority**" means the Independent Broadcasting Authority established by the Independent Broadcasting Authority Act, 2002;

[Act No. 17 of 2002]

"**information system**" means a system for the generation, sending, reception, storage, display or other processing of data messages, and includes the internet;

"**joint controllers**" means two or more data controllers who jointly determine the purposes for which and the means by which personal data is processed;

"**law enforcement officer**" means—

(a) a police officer above the rank of sub-inspector;

(b) an officer of the Anti-Corruption Commission;

(c) an officer of the Drug Enforcement Commission;

(d) an officer of the Zambia Security Intelligence Service; and

(e) any other person appointed by the Minister for purposes of this Act;

"**legally disqualified**" has the meaning assigned to the words in the Mental Health Act, 2019;

[Act No. 6 of 2019]

"**legal practitioner**" has the meaning assigned to the words in the Legal Practitioners Act;

[Cap. 30]

"**meta data**" means data that describes other data;

"**personal data**" means data which relates to an individual who can be directly or indirectly identified from that data which includes a name, an identification number, location data, an online identifier, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

"**processing**" means an operation or a set of operations which is or are performed on personal data, whether or not by automatic means, including the collection, recording or holding of the data or the carrying out of any operation or set of operations on data, including—

(a) organisation, adaptation or alteration of the data;

(b) retrieval, consultation or use of the data;

(c) alignment, combination, blocking, erasure or destruction of the data; or

(d) disclosure of the information or data by transmission, dissemination or otherwise making available;

"**profiling**" means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, including analysis or prediction of the data subject's aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;

"**pseudonymisation**" means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, where that additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data is not attributed to an identified or identifiable natural person;

"**public body**" has the meaning assigned to the words in the Public Finance Management Act, 2018;

[Act No. 1 of 2018]

"**recipient**" means a person to whom data is disclosed, including an employee or agent of a data controller, a data processor or an employee or agent of a data processor in the course of processing the data for the data controller, but does not include a person to whom disclosure is or may be made as a result of, or with a view to, a particular inquiry by or on behalf of that person made in the exercise of any power conferred by law;

"**Register**" means the Register kept and maintained under section 80;

"**sensitive personal data**" means personal data which by its nature may be used to suppress the data subject's fundamental rights and freedoms and includes

(a) the race, marital status, ethnic origin or sex of a data subject;

(b) genetic data and biometric data;

(c) child abuse data;

(d) a data subject's political opinions;

(e) a data subject's religious beliefs or other beliefs of a similar nature;

(f) whether a data subject is a member of a trade union; or

(g) a data subject's physical or mental health, or physical or mental condition;

"**third party**" means a person other than—

(a) a data subject;

(b) a data controller, or

(c) a data processor or other person authorised to process data on behalf of data controller or data processor.

"**vulnerable person**" means a person aged 18 or above and whose ability to make informed decisions about their rights and well being is temporally or permanently impaired through physical or medically certified hindrance or impairment; and

3. Application

(1) This Act applies to the processing of personal data performed wholly or partly by automated means and to any processing otherwise than by electronic means.

(2) This Act does not apply to the processing of personal data by an individual for personal use.

Part II – Office of the Data Protection Commissioner

4. Establishment of Office of Data Protection Commissioner

(1) There is established in the Ministry responsible for communications the Office of the Data Protection Commissioner which is responsible for the regulation of data protection and privacy in the Republic.

(2) The functions of the Office of the Data Protection Commissioner are to—

(a) register controllers and data processors;

(b) licence data auditors;

(c) disseminate information and promotion of the participation of stakeholders in the process of data protection in the Republic;

(d) advise Government on matters relating to data protection;

(e) keep and maintain a register of data controllers, data processors and data auditors;

(f) represent Government internationally on matters relating to data protection;

(g) conduct research and development relating to data protection;

(h) ensure proper and effective coordination and collaboration with similar regional and international authorities;

(i) receive and investigate complaints under this Act; and

(j) vary conditions and terms of a licence issued under this Act.

5. Data Protection Commissioner

(1) The President, through the Civil Service Commission, shall appoint a Data Protection Commissioner who shall be a public officer with the following skills, qualifications and expertise:

(a) minimum university degree level in information communication technologies;

(b) data protection rules and operations;

(c) data protection laws; and

(d) at least four years at senior management level in a related field.

(2) The Data Protection Commissioner is responsible for the day to day administration of the Office of the Data Protection Commission.

6. Appointment of Deputy Data Protection Commissioners and other staff

(1) The Civil Service Commission shall, on the recommendation of the Office of the Data Protection Commissioner, appoint as public officers two Deputy Data Protection Commissioners and other staff as may be necessary for the performance of the functions of the Office of the Data Protection Commission.

(2) The two Deputy Data Protection Commissioners are responsible for the formulation of policies and planning and for data processing system.

Part III – Inspectorate

7. Inspector

(1) The Civil Service Commission may appoint a suitably qualified person to be an inspector for the purposes of ensuring compliance with this Act.

(2) The Civil Service Commission shall issue an inspector with an identification card and a certificate of appointment in the prescribed form which are *prima facie* evidence of the inspector's appointment.

8. Power of inspectors

(1) An inspector may, for the purpose of enforcing the provisions of this Act, at any reasonable time and with a warrant—

(a) enter and inspect the business premises of a data controller or data processor;

(b) inspect equipment and supplies in or about the licensed premises;

(c) have access to and inspect, examine and audit documents, books and records of the data controller or data processor;

(d) remove a document, book, record or other document which an inspector believes may afford evidence of offence under this Act;

(e) require from a data controller or data processor an explanation of any record or entry in the document, book, record or other document;

(f) make copies of or extracts from, a document, book, record or other document relating to the licensed activity on any premises that has a bearing on an investigation; and

(g) remove from the premises any equipment, commodity or product used in contravention of this Act.

(2) An inspector may perform an inspection for the purposes of ensuring a data controller's or data processor's compliance with this Act.

(3) A data controller or data processor shall afford an inspector access to any record or document for purposes of an inspection and produce to the inspector, a record or document that the inspector may require.

(4) An inspector shall exercise the power under subsection (1)(a) in relation to a dwelling house or any land or building occupied as a private dwelling, during the day with a warrant.

(5) An inspector who removes an article, document, record, book or any other thing from any premises under subsection (1), shall—

(a) issue a receipt for the article, document, record, book or any other thing to the owner or person in control of the premises; and

(b) return the article, thing, record, book or any other document as soon as practicable after achieving the purpose for which it was removed.

9. Arrest without warrant

(1) An inspector may arrest a person, without a warrant, where the inspector has reasonable grounds to believe that the person—

(a) has committed an offence under this Act;

(b) is about to commit an offence under this Act and there is no other way to prevent the commission of the offence; or

(c) is willfully obstructing an inspector in the execution of the inspector's duties.

(2) An inspector who makes an arrest under subsection (1) shall, without delay, have the person arrested brought to a police station.

10. Seizure of property

A law enforcement officer may seize and detain property which the inspector has reason to believe was used to commit an offence under this Act until an order of the court is made regarding the disposal thereof.

11. Restoration of property

(1) A law enforcement officer shall, where a person from whom an article or other property has been seized under section 10 is found not guilty or the proceedings against that person are withdrawn—

(a) without delay, restore the article or property to that person; or

(b) where the enforcement officer is satisfied that the person cannot be found or is unwilling to receive back the article or property, apply to the court for an order of forfeiture of the article or property.

(2) The court shall make an order of forfeiture under subsection (1) if—

(a) the law enforcement officer has given notice, by publication in the *Gazette* and in a daily newspaper of general circulation in the Republic, to the effect that the article or property which has been seized under this Act shall vest in the State if it is not claimed within three months from the date of publication of the notice; and

(b) three months after the giving of the notice under paragraph (a), the article or property remains unclaimed.

(3) Where a claim is made, in writing, by a person that is lawfully entitled to the article or property seized under this Act, the law enforcement officer may order the release of the article or property to the claimant if satisfied that there is no dispute concerning the ownership of the article or property and that it is not liable to forfeiture.

Part IV – Principles and rules relating to processing of personal data

12. Principles relating to processing of personal data

(1) A data controller or data processor shall ensure that personal data is—

(a) processed lawfully, fairly and transparently;

(b) collected for explicit, specified and legitimate purposes and not further processed in a manner incompatible with those purposes;

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed;

(d) accurate and where necessary, kept up to date, with every reasonable step taken to ensure that any inaccurate personal data is erased or rectified without delay;

(e) stored in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed;

(f) processed in accordance with the rights of a data subject; and

(g) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against any loss, destruction or damage, using appropriate technical or organisational measures.

(2) For the purposes of subsection 1(b), processing of personal data for purposes of archiving in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purpose.

13. Processing of personal data

Subject to the other provisions of this Act, a data controller may process personal data where—

(a) the data subject has given consent to the processing of that data subject's personal data;

(b) the processing is necessary—

(i) for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

(ii) for compliance with a legal obligation to which the data controller is subject;

(iii) in order to protect the vital interests of the data subject or of another natural person;

(iv) for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller;

(v) for the purposes of the legitimate interests pursued by the data controller or by a third party, except where such interests are overridden by the interest or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child; or

(c) the processing relates to personal data which is manifestly made public by the data subject.

14. Processing of sensitive personal data

(1) A person shall not process sensitive personal data, unless—

(a) processing is necessary for the establishment, exercise or defence of a legal claim or whenever a court is exercising a judicial function;

(b) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services; or

(c) processing is necessary for reasons of public interest.

(2) Personal data under subsection (1)(b) may be processed when the data is processed by or under the responsibility of a professional, subject to secrecy and other obligations imposed by any law or professional bodies regulating them.

(3) Personal data referred to under subsection (1)(c) shall be processed only where adequate measures to safeguard the rights and freedoms of the data subject have been put in place.

15. Consent, justification and objection

(1) A data controller shall not process personal data unless the data subject consents to the processing.

(2) A data subject may consent to the processing of that data subject's personal data in writing.

(3) Prior to giving consent, the data subject shall be informed of the data subject's right to withdraw the consent.

(4) A data controller shall, where processing is based on consent, demonstrate that the data subject has consented to the processing.

(5) Where a data subject consents in the form of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language.

(6) A data subject shall have the right to withdraw consent at any time.

(7) The withdrawal of consent shall not affect the lawfulness of processing based on consent under subsection (5) before its withdrawal and all personal data collected following withdrawal of the consent shall, subject to the provisions of this Act, be destroyed immediately.

(8) A data subject may object, at any time, to the processing of that data subject's personal data.

(9) Where a data subject has objected to the processing of that data subject's personal data, the data controller or data processor shall no longer process that personal data.

16. Collection of personal data

(1) Subject to subsection (2), a data controller shall collect personal data directly from a data subject.

(2) A data controller may collect personal data from a source other than the data subject if—

(a) the data is contained in or derived from a public record or has intentionally been made public by the data subject;

(b) the data subject has consented to the collection of data from another source;

(c) collection of data from another source would not prejudice the interest of the data subject;

(d) collection of data from another source is necessary—

(i) to avoid prejudice to the maintenance of the law and order by any public body, including the prevention, detection, investigation, prosecution and punishment of an offence;

(ii) to comply with an obligation imposed by law; or

(iii) for the conduct of proceedings in any court or tribunal that have commenced or are reasonably contemplated; or

(iv) for the purposes of national security;

(e) collection from the data subject would prejudice a lawful purpose of the collection;

(f) compliance is not reasonably practicable in the circumstances of the particular case; or

(g) it is—

(i) necessary for the provision of an emergency medical service to the data subject;

(ii) required for the establishment of the identity of the data subject and the collection is authorised by a law written for that purpose;

(iii) necessary to prevent a reasonable threat to national security, defence or public order; or

(iv) necessary to prevent, investigate or prosecute a cognisable offence.

17. Processing of child and vulnerable person's personal data

(1) Where a data subject is a child or a vulnerable person, that data subject's right may be exercised by that data subject's parents, legal guardian or a person exercising parental responsibility as the case may be.

(2) A data controller shall not process a child's or vulnerable person's personal data unless consent is given by the child's or vulnerable person's parent, legal guardian or a person exercising parental responsibility.

(3) A data controller shall, where the personal data of a child or a vulnerable person is involved, make every reasonable effort to verify that consent has been given or authorised, taking into account available technology.

(4) A data controller shall incorporate appropriate mechanisms for age verification and parental consent in the processing of personal data of a child.

18. Offence and penalty for contravention of personal data obligation

(1) A body corporate that contravenes the provisions of this Part commits an offence and is liable on conviction to—

(a) a fine not exceeding one hundred million penalty units; or

(b) two percent of annual turnover of the preceding financial year, whichever is higher.

(2) Where the offence is committed by a natural person, that person shall be liable, on conviction to a fine not exceeding one million penalty units or to imprisonment for a term not exceeding five years, or to both.

Part V – Regulation of data controllers, data processors and data auditors

19. Prohibition from controlling or processing personal data without registration

(1) A person shall not control or process personal data without registering as a data controller or a data processor under this Act.

(2) A person who contravenes subsection (1) commits an offence and is liable, on conviction to a fine not exceeding five hundred thousand penalty units or to imprisonment for a term not exceeding five years or both.

20. Application for registration as data processor or data controller

(1) A person who intends to process personal data shall apply to the Data Protection Commissioner for registration as a data controller or data processor in a prescribed manner and form on payment of a prescribed fee.

(2) The Data Protection Commissioner may, within fourteen days of receipt of an application under subsection (1), grant or reject the application.

(3) The Data Protection Commissioner shall, where it rejects an application under subsection (2), inform the applicant, in writing and give reasons for the decision.

21. Registration of data controller and data processor

(1) The Data Protection Commissioner shall, within fourteen days of the approval of an application under section 20, issue the applicant with a certificate of registration, if the applicant meets the prescribed requirements.

(2) A registered data controller or data processor shall display the certificate of registration issued under this Act in a conspicuous place at the registered data controller's or data processor's principal place of business and a certified copy of the certificate of registration at every subsidiary premises where the registered data controller or data processor carries on business.

22. Renewal of certificate of registration

(1) A registered data controller or data processor may three months before the expiration of the validity of the certificate, apply to the Authority for renewal of a certificate of registration in a prescribed manner and form on payment of a prescribed fee.

(2) The Data Protection Commissioner shall, within thirty days of receiving an application for the renewal of a certificate of registration, approve or reject the application and give reasons where it rejects the application for renewal of the certificate.

(3) A holder of a certificate of registration who submits an application for the renewal of a certificate of registration in accordance with subsection (1), shall continue to operate the business or activity until a decision is made by the Data Protection Commissioner on the application.

23. Change in details of data controller or data processor

A registered data controller or data processor under this Act shall notify the Data Protection Commissioner of any change in the particulars relating to the registration within seven days of the change.

24. Suspension or cancellation of registration

(1) Subject to other provisions of this Act, the Data Protection Commissioner may suspend or cancel the registration of a data controller or data processor if the registered data controller or data processor—

(a) obtained the registration on the basis of fraud, misrepresentation or concealment of a material fact;

(b) has ceased to carry on business in the data processing or controlling industry for a prescribed period;

(c) fails to comply with any term or condition of the certificate of registration; or

(d) operates the registered business activity in contravention of this Act or any other relevant written law.

(2) The Data Protection Commissioner shall, not less than thirty days before suspending or cancelling registration of a data controller or data processor in accordance with subsection (1), notify the registered data controller or data processor of the intention to suspend or cancel the registration giving reasons for its decision and requesting the registered data controller or data processor to show cause, within a period as the Data Protection Commissioner shall specify in the notice, why the registration of the data controller or data processor shall not be suspended or cancelled.

(3) Where the Data Protection Commissioner is not satisfied with the reasons advanced by the data controller or data processor under subsection (2), the Data Protection Commissioner shall proceed to suspend or cancel, the registration stating the reasons for the suspension or cancellation.

(4) Where a certificate of registration is cancelled or suspended, the Data Protection Commissioner shall prescribe conditions with which the data collected from the data subjects will be processed.

(5) A data controller or data processor who contravenes subsection (4) commits an offence and is liable, on conviction, to a fine not exceeding one million penalty units or to imprisonment for a term of five years.

25. Re-registration

Where a certificate of registration is cancelled or suspended under section 24, the holder of the certificate of registration may apply to the Data Protection Commissioner for re-registration in a prescribed form and manner on payment of a prescribed fee.

26. Surrender of certificate of registration

(1) Where a registered data controller or data processor decides not to continue providing the services, the data controller or data processor shall notify the Data Protection Commissioner in writing.

(2) The Data Protection Commissioner shall prescribe terms and conditions on which the certificate of registration shall be surrendered.

(3) Where a certificate of registration is surrendered under sub section (1), the certificate of registration shall lapse, and the data controller or data processor shall cease to be entitled to any benefits obtainable under the certificate of registration.

(4) A data controller or data processor who fails to adhere to the terms and conditions of surrender in subsection (2) commits an offence and is liable, on conviction, to a fine not exceeding one million penalty units or to imprisonment for a term of ten years.

27. Exemption from registration

The Data Protection Commissioner may, by declaration, exempt a person for a limited or unlimited period of time, from the requirement to hold a certificate of registration to process personal data.

28. Power to forbear

(1) The Data Protection Commissioner may forbear from applying to a data controller any provision of this Part, where the Data Protection Commissioner considers that forbearance is consistent with the objects of this Act.

(2) The Data Protection Commissioner shall, where it decides to forbear from applying any provision, immediately, publish a notice of forbearance in the *Gazette*, setting out the details of and the reasons for, the decision.

Part VI – Data auditors

29. Data auditors

The Data Protection Commissioner shall licence data auditors in the prescribed manner and form on payment of the prescribed fee.

30. Application for licence

(1) A person who intends to provide data auditing services under this Act shall apply to the Data Protection Commissioner for a licence in the prescribed manner and form on payment of the prescribed fee.

(2) The Data Protection Commissioner shall, within sixty days of receipt of an application, grant or reject the application.

(3) Where the Data Protection Commissioner fails to make a decision within the period referred to under subsection (2), except as otherwise provided under this Act, the application shall be deemed to have been granted.

(4) The Data Protection Commissioner shall, where it rejects an application for a licence, inform the applicant in writing stating the reasons for the rejection.

(5) The Data Protection Commissioner may request for further particulars in respect of an application.

(6) Where the Data Protection Commissioner requests for particulars referred to in subsection (5), the period referred to in subsection (2) stops running.

31. Issue of licences

A licence under this Act shall only be issued to an applicant that possesses the relevant technical capabilities determined by the Data Protection Commissioner.

32. Conditions of licence

A licence issued under this Act shall—

(a) contain the terms and conditions of the licence; and

(b) be valid for the period as maybe prescribed.

33. Variation of licence

(1) A licensee may, at any time during the validity of the licence, apply to the Data Protection Commissioner for variation of the terms and conditions of the licence or any matter relating to the licence.

(2) The Data Protection Commissioner shall consider the application referred to in subsection (1) and may grant or reject the application, and shall give reasons to the applicant where it rejects the application.

(3) The Data Protection Commissioner may vary the licence or the terms and conditions of a licence where—

(a) the variation is necessary in the public interest; or

(b) the variation is necessary to address the concerns of the members of the public;

(4) The Data Protection Commissioner shall, before making any variation of the terms and conditions of a licence under this section, give notice to the licensee—

(a) stating that it proposes to make variations in the manner specified in the notice; and

(b) specifying the time, not being more than fourteen days from the date of service of the notice on the Licensee, within which written representation in respect of the proposed variation may be made to the Data Protection Commissioner by the licensee.

(5) Compensation shall not be payable by the Data Protection Commissioner to a licensee for any variation to a licence.

34. Surrender of licence

(1) Where a licensee decides not to continue providing the services relating to the licence, the licensee shall notify the Data Protection Commissioner in writing and shall agree with the Data Protection Commissioner on the terms and conditions of the surrender of the licence, with particular reference to anything done or any benefit obtained under the licence.

(2) Where a licence is surrendered under sub section (1), the licence shall lapse, and the licensee shall cease to be entitled to any benefits obtainable under the licence.

(3) Where a licence is surrendered under subsection (1), the licensee shall not be entitled to a refund of any fees paid with respect to the licence.

35. Transfer or licence

(1) A licensee shall not cede, pledge, encumber or otherwise dispose of a licence.

(2) A licensee may transfer or assign a licence with the prior approval of the Data Protection Commissioner.

(3) An application for approval to transfer or assign a licence shall be made to the Data Protection Commissioner.

(4) The Data Protection Commissioner may, within thirty days of receipt of the application—

(a) approve the application on such terms and conditions as it may determine; or

(b) reject the application in accordance with the provisions of this Act.

36. Suspension and cancellation

(1) Subject to the other provisions of this Act, the Data Protection Commissioner may suspend or cancel a licence if the holder:

(a) obtained the licence by fraud or submission of false information or statements;

(b) contravenes this Act, any other written law relating to the licence or any terms and conditions of the licence;

(c) fails to comply with a decision or guidelines issued by the Data Protection Commissioner;

(d) enters into receivership or liquidation or takes any action for voluntary winding up or dissolution;

(e) enters into any scheme of arrangement, other than for the purpose of reconstruction or amalgamation, on terms and within such period as may previously have been approved in writing by the Data Protection Commissioner;

(f) is the subject of any order that is made by a court or tribunal for its compulsory winding up or dissolution;

(g) has ceased to fulfil the eligibility requirements under this Act; or

(h) the suspension or cancellation is in the public interest.

(2) The Data Protection Commissioner shall before suspending or cancelling the licence in accordance with this section, give written notice to the holder thereof of its intention to suspend or cancel the licence and shall—

(a) give the reasons for the intended suspension or cancellation; and

(b) require the holder to show cause, within a period of not more than thirty days, why the licence should not be suspended or cancelled.

(3) The Data Protection Commissioner shall not suspend or cancel a licence under this section if the licensee takes remedial measures to the satisfaction of the Data Protection Commissioner within the period referred to in subsection (2).

(4) The Data Protection Commissioner shall, in making its final determination on the suspension or cancellation of the licence consider submissions made by the licensee under subsection (2).

(5) The Data Protection Commissioner may suspend or cancel a licence if the holder after being notified under subsection (2) fails to show cause or does not take remedial measures, to the satisfaction of the Data Protection Commissioner within the time specified in that subsection.

(6) The Data Protection Commissioner shall, where it suspends or cancels a licence under this section, publish the suspension or revocation in the Register.

37. Renewal of licence

(1) A licensee may, not less than three months before the expiry of a licence, apply for a renewal of the licence in the prescribed manner and form on payment of a prescribed fee.

(2) The Data Protection Commissioner shall, where a licensee makes an application under subsection (1), renew the licence if the licensee—

(a) fulfils the eligibility requirements as prescribed under this Act;

(b) at the time of the renewal, the licensee is compliant with the terms and conditions of the licence, the Guidelines issued by the Data Protection Commissioner or any other relevant law.

(3) Where the Data Protection Commissioner rejects an application for renewal of a licence, the Data Protection Commissioner shall inform the licensee and give reasons for the rejection.

38. Functions of data auditor

The functions of a data auditor are to—

(a) promote adherence to principles of data protection by controllers and processors of data;

(b) ensure that data controllers and data processors implement adequate policies and procedures to regulate the processing of personal data;

(c) enhance public and stakeholder awareness of data protection principles and rights; and

(d) check that data controllers implement adequate safeguards to prevent data leaks and data breaches from data controllers and data processors.

Part VII – Exemptions from principles and rules of processing of data

39. National security, defence and public order

A data controller that processes personal data in the interests of national security, defence and public order is exempt from the provisions of part IV, except for section 12(1)(c), (d), (e) and (g).

40. Prevention, detection, investigation and prosecution of contraventions of law

(1) The processing of personal data in the interests of prevention, detection, investigation and prosecution of an offence or any other contravention of law shall not be permitted unless it is authorised by a written law and is necessary for, and proportionate to, such interests being achieved.

(2) Processing authorised by law under subsection (1) shall be exempt from the provisions of Part IV, except section 12(1)(c), (d), (e) and (g).

(3) A data controller shall not retain personal data processed under subsection (1) once the purpose of prevention, detection, investigation or prosecution of an offence or other contravention of law is complete except where that personal data is necessary for the maintenance of any record or database which constitutes a proportionate measure to prevent, detect, investigate or prosecute an offence or class of offences in future.

41. Processing for purposes of legal proceedings

(1) Where processing of personal data is necessary for enforcing a legal right or claim, seeking a relief, defending a charge, opposing a claim, or obtaining legal advice from a legal practitioner in an impending legal proceeding, that processing shall be exempt from the provisions of Part IV except section 12(1)(c), (d), (e) and (g).

(2) Where processing of personal data by a court or tribunal is necessary for the exercise of any judicial function, that processing is exempt from the provisions of part IV except section 12(1)(c), (d), (e) and (g).

42. Research, archiving or statistical purposes

(1) Where processing of personal data is necessary for research, archiving, or statistical purposes, that processing is exempt from the provisions of Part IV, except section 12 (1)(c), (d), (e) and (g).

(2) Despite subsection (1), where sensitive personal data is being processed for research purposes that relate to scientific or historical research by a person other than a public body, that person shall not process such sensitive personal data without the authorisation of the Data Protection Commisioner.

(3) Where personal data is being processed for scientifc research purposes by a person other than a public body, that person shall ensure that the personal data is anonymised

43. Journalistic purpose

(1) Where the processing of personal data is necessary for or relevant to a journalistic purpose, that processing is exempt from the provisions of the Act, except—

(a) section 12(l)(c), (d), (e) and (g); and

(b) section 47.

(2) Subsection (1) applies only where a data controller can demonstrate that the processing is in compliance with—

(a) the law regulating journalists in the Republic, or

(b) any code or guidelines issued by the Independent Broadcasting Authority.

44. Processing to be lawful and legitimate

The requirement for the processing of personal data under this Part shall be for the lawful and legitimate purposes.

Part VIII – Duties of data controller and data processor

45. Record of processing activities

(1) A data controller shall keep and maintain, in writing, a record of—

(a) processing activities and meta data under its responsibility in the prescribed manner and form; and

(b) all categories of processing activities carried out in the prescribed manner and form.

(2) A data controller shall make the record available to the Data Protection Commissioner on demand.

46. Data protection impact assessment

(1) A data controller shall, where a type of processing uses new technologies, taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of an individual, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.

(2) A data protection impact assessment under subsection (1) is required where—

(a) personal data is procecessed using an automated processing system, including profiling, which produces legal effects concerning the natural person or similarly significantly affects that natural person;

(b) processing on a large scale of sensitive personal data, or of personal data relating to criminal convictions and offences; or

(c) a systematic monitoring of a publicly accessible area on a large scale.

(3) Despite subsection (2), the Data Protection Commissioner shall establish and make public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment under subsection (1).

(4) An impact assessment under subsection (1) shall be in a prescribed manner and form.

(5) A data controller shall, where necessary, carry out a review to assess if processing is performed in accordance with the data protection impact assessment where there is a change of the risk represented by processing operations.

47. Security of processing

(1) A data controller or data processor, shall provide guarantees regarding the technical and organisational security measures employed to protect the personal data associated with the processing undertaken and ensure strict adherence to such measures.

(2) A data controller or the data processor shall, having regard to the nature, scope and purpose of processing personal data undertaken, the risks associated with such processing, and the likelihood

and severity of the harm that may result from such processing, implement appropriate security safeguards including—

(a) maintaining integrity of personal data using methods including pseudonymisation and encryption;

(b) ensuring ongoing confidentiality, integrity and implementation of measures necessary to protect the integrity of personal data;

(c) measures necessary to prevent misuse, unauthorized access to, modification, disclosure or destruction of personal data; and

(d) implementation of appropriate data protection policies.

(3) A data controller and data processor shall undertake a periodic review of security safeguard in accordance with guidelines issued by the Data Protection Commissioner.

(4) Where processing is to be carried out on behalf of a data controller, the data controller shall only use processors providing sufficient guarantees to implement appropriate technical and organisational measures in a manner that ensures that the processing will meet the requirements of this Act and protect the rights of the data subject.

48. Appointment of data protection officer

(1) Subject to subsection (2), a data controller and data processor shall appoint a data protection officer.

(2) A data protection officer shall be appointed in accordance with the guidelines issued by the Data Protection Commissioner.

49. Notification of security breach

(1) A data controller shall notify the Data Protection Commissioner within twenty-four hours of any security breach affecting personal data processed.

(2) A data processor shall notify the data controller, as soon as practicable of any security breach affecting personal data processed on behalf of the data controller.

(3) A data controller or data processor shall notify the data subject, as soon as practicable of any security breach affecting personal data processed.

50. Accountability

A data controller and data processor shall—

(a) take necessary measures to comply with the principles and obligations specified in this Act; and

(b) have the necessary internal mechanisms in place for demonstrating such compliance to both data subjects and to the Data Protection Commissioner.

51. Data retention

(1) Subject to the provisions of this Act, a data controller and data processor shall keep personal information for as long as that personal information is used for the specific purpose for which the personal information was collected and for as long as the personal information is relevant for that purpose and for a period of at least one year thereafter or other period that may be prescribed.

(2) A data controller and a data processor shall keep a record of the process and a record of the purpose for which the personal information was collected and third parties to whom and when the personal information was disclosed.

52. Duties of data processor

(1) A data processor shall not engage another data processor without prior specific or general written authorisation of the data controller.

(2) A data processor shall, where a data controller is granted general authorisation to engage another data processor, inform the data controller of any intended changes concerning the addition or replacement of other data processors, thereby giving the data controller the opportunity to object to those changes.

(3) Processing by a data processor shall be governed by a contract that sets out the subject matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects, the obligations and rights of the controller and any other matter, as prescribed.

(4) The Data Protection Commissioner may, for the purposes of this section, issue guidelines specifying further obligations and any other matters regarding data processors.

53. Non-disclosure of personal data

(1) Except as otherwise provided in this Act, a person shall not disclose or otherwise cause any other person to receive the content or nature of any personal data that has been collected.

(2) Subject to subsection (3), a data controller or data processor who seeks to disclose personal data shall, prior to its disclosure, obtain the consent of the data subject.

(3) A data controller or data processor, who seeks to disclose personal data, shall inform the data subject, prior to a disclosure of personal data under this section, of the following details in respect of the data subject's personal data:

(a) when and to whom it will be disclosed;

(b) the purpose of its disclosure;

(c) the security practices, privacy policies and other policies, if any, that will protect it; and

(d) the procedure for recourse in case of any grievance in relation to it.

(4) A data controller or data processor shall not disclose, without consent of the data subject, personal data unless it is necessary to prevent—

(a) a reasonable threat to national security, defence or public order; or

(b) investigate or prosecute a cognisable offence.

(5) A person who contravenes a provision of this section commits an offence and is liable on conviction to a fine not exceeding two hundred thousand penalty units or to imprisonment for a term not exceeding two years or to both.

54. Joint controllers

(1) Where two or more data controllers jointly determine the purposes and means of processing data, the joint controllers shall enter into an agreement which reflects the respective roles and relationships of the joint controllers' as they relate to the data subject.

(2) An agreement entered into under subsection (1) shall be made available to the data subject.

(3) Joint data controllers shall be jointly and severally liable to the data subject.

55. Offence by data controller

(1) A body corporate that contravenes the provisions of this part commits an offence and is liable, on conviction, to two percent of annual turnover of the preceding financial year or to two million penalty units, whichever is higher.

(2) Where an offence under subsection (1) is committed by a natural person, that person shall be liable, on conviction, to a fine not exceeding one million penalty units or to imprisonment for a term not exceeding ten years, or to both.

56. Personal data in legal proceedings

A person shall not process personal data in legal proceedings, except—

(a) under the supervision of a public body discharging its duty if the processing is necessary for those legal proceedings;

(b) where the processing is necessitated by litigation; or

(c) by a legal practitioner to the extent that the processing is necessary for the protection of the legal practitioner's clients' interests.

57. Notification

A data controller or data processor shall notify the Data Protection Commissioner of any third party agreement that allows the third party to trade on the profile of a data subject.

Part IX – Rights of the data subject

58. Right of access and notification

(1) A data subject has the right to obtain from the data controller, confirmation as to whether or not personal data concerning that data subject is being processed.

(2) A data subject may, where that data subject's personal data is being processed, access in a manner that the data subject understands the following information:

(a) the purpose of the processing, the category of data the processing relates to, and the categories of recipients the data is disclosed to;

(b) envisaged period for which the personal data shall be stored, where possible or if not possible, the criteria used to determine that period;

(c) data being processed, as well as the source of that data; and

(d) information about the basic logic involved in any automatic processing of data relating to the data in case of automated decision making.

(3) A data subject has the right to notification of all third parties to whom that data subject's personal data has been disclosed and the measures put in place to safeguard personal information of that data subject.

(4) A data subject shall access that data subject's personal data in accordance with the relevant written law relating to access to information.

(5) Where sensitive personal data is processed for the purpose of scientific research, informing the data subject may be postponed until the research is concluded, if—

(a) informing the data subject would significantly prejudice the research;

(b) there is no evident risk of infringement of the data subject's right to protection of the data subject's privacy; and

(c) the data was collected initially on the basis of consent.

(6) A data controller may provide a copy of the personal data undergoing processing at no cost for the initial data and at a reasonable fee based on administrative costs for additional copies of the data.

(7) Where the data subject makes a data request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic format.

(8) The right to obtain a copy of personal data under subsection (5) shall not be enforced where that enforcement prejudices the rights and freedoms of others.

59. Right to rectification

(1) The data subject has the right to, rectification of inaccurate personal data concerning the data subject as soon as practicable.

(2) A data subject shall taking into account the purposes of the processing, have the right to have incomplete personal data completed.

60. Right to erasure

(1) The data subject has the right to erasure of personal data of that data subject as soon as practicable and the data controller shall have the obligation to erase personal data without undue delay where the—

(a) personal data is no longer necessary in relation to the purposes for which it was collected or otherwise processed;

(b) data subject, or a person holding parental responsibility, where the data subject is a child, withdraws consent and there is no other legal ground for the processing;

(c) data subject objects to the processing and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing unless the data controller is otherwise permitted by the provisions of this Act;

(d) personal data has been unlawfully processed; or

(e) personal data has to be erased for compliance with a legal obligation in the Republic to which the data controller is subject.

(2) A data controller shall, where the data controller has made the personal data public, take all reasonable steps to inform a data processor and third party processing that data by virtue of that publication, that the data subject has requested the erasure of any links to, or copy or replication of, that personal data.

61. Right of objection

(1) Subject to this Act, a data subject may object, to processing of that data subject's personal data.

(2) A data controller shall not, where a data subject objects to the processing of that data subject's personal data, process the personal data objected to under subsection (1) unless the data controller is permitted by the provisions of any other written law.

(3) A data subject may, where personal data is processed for direct marketing purposes, object to processing of that data subject's personal data.

(4) Where a data subject objects to the processing of personal data for direct marketing purposes, the personal data shall no longer be processed for that purpose but may be processed for any other lawful purpose.

(5) A data controller shall on the first communication with the data subject, expressly bring the rights of the data subject to the attention of the data subject and present the information clearly and separately from any other information.

62. Decision taken on basis of automatic data processing

(1) A data subject shall not be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning that data subject or similarly affects that data subject.

(2) Subsection (1) shall not apply if the decision is—

(a) necessary for entering into, or performance of, a contract between the data subject and a data controller;

(b) authorised by any written law; or

(c) based on the data subject's explicit consent.

(3) A data controller shall, in cases under subsection (2), implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, including the right to obtain human intervention on the part of the data controller for purposes of enabling the data subject to express the data subject's point of view and contest the decision.

(4) Automated data processing shall not be undertaken where the processing involves sensitive personal data unless—

(a) the data subject has expressly consented to that processing;

(b) the processing is in the public interest; or

(c) the processing is permitted by any written law and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.

63. Right to restriction of processing

(1) A data subject may restrict a data controller from processing that data subject's personal data where the—

(a) accuracy of the personal data is contested by the data subject, for a period enabling the data controller to verify the accuracy of the personal data;

(b) data controller no longer needs the personal data for the purposes of the processing, but it is required by the data subject for the establishment, exercise or defence of legal claims;

(c) data subject has objected to processing pursuant to section 60(1)(c) pending the verification whether the legitimate grounds of the data controller override those of the data subject.

(2) Where processing has been restricted under subsection (1), that personal data shall, with the exception of storage, only be processed with the data subject's consent or for the establishment, exercise or defence of legal claims or for reasons of important public interest or where the law compels that processing.

(3) A data subject who has obtained a restriction on the processing of that data subject's personal data pursuant to subsection (1) shall be informed by the data controller before the restriction of processing that data is lifted.

64. Information when personal data collected directly from data subject

A data controller shall where personal data relating to the data subject is collected directly from the data subject, concurrently provide the data subject with the following information, unless it is established that the data subject is in receipt of that information:

(a) the name and address of the data controller;

(b) the purpose of the processing;

(c) if it is obtained for the purpose of direct marketing, existence of the right to object, to the intended processing of personal data relating to that data subject;

(d) where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the safeguards put in place for that transfer;

(e) whether compliance with the request for information is compulsory or not, as well as what the consequences of the failure to comply are;

(f) taking into account the specific circumstances in which the data is collected, any supporting information, as necessary to ensure fair processing for the data subject, such as—

(i) the recipients or categories of recipients of the data; and

(ii) the existence of the right to access and rectify the personal data relating to that data subject, except where that additional information, taking into account the specific circumstances in which the data is collected, is not necessary to guarantee accurate processing.

65. Right to data portability

(1) A data subject has the right to receive that data subject's personal data in a structured, commonly used, machine readable or otherwise legible format and may transmit that data to another data controller

(2) A data subject has the right to have the data subject's personal data transmitted directly from one data controller to another, where technically or otherwise feasible.

66. Notification obligation

A data controller shall communicate any rectification or erasure of personal data or restriction of processing carried out in accordance with this Act to each recipient to whom the personal data have been disclosed, where practicable.

67. Derogation from rights

The rights of a data subject under this Part shall, to the extent necessary, not apply where processing is—

(a) for compliance with a legal obligation which requires processing by any written law to which the data controller is subject;

(b) for the performance of a task carried out in the public interest;

(c) in the exercise of official authority vested in the data controller;

(d) for scientific or historical research purposes; or

(e) for the establishment, exercise or defence of legal claims.

68. Complaints

A data subject may lodge a complaint with the Data Protection Commissioner if the data subject considers that the processing of personal data by a data controller or data processor contravenes this Act.

69. Appeals

A person who is aggrieved with the decision of the Data Protection Commissioner may appeal to the High Court within thirty days of the Data Protection Commission's decision.

Part X – Transfer of personal data outside the Republic

70. Cross-border transfer of personal data

(1) A data controller shall process and store personal data on a server or data centre located in the Republic.

(2) Despite subsection (1), the Minister may prescribe categories of personal data that may be stored outside the Republic.

(3) Despite subsection (2), sensitive personal data shall be processed and stored in a server or data centre located in the Republic.

71. Conditions for cross-border transfer of personal data

(1) Personal data other than personal data categorised in accordance with section 70(2) may be transferred outside the Republic where—

(a) the data subject has consented and

(i) the transfer is made subject to standard contracts or intragroup schemes that have been approved by the Data Protection Commissioner; or

(ii) the Minister, has prescribed that transfers outside the Republic is permissible; or

(b) the Data Protection Commissioner approves a particular transfer or set of transfers as permissible due to a situation of necessity.

(2) The Minister may, by statutory instrument, prescribe the criteria for cross border data transfers under subsection (l)(a)(ii) where the Minister considers that—

(a) the relevant personal data shall be subject to an adequate level of protection, having regard to the applicable laws and international agreements; and

(b) the enforcement of data protection laws by authorities with appropriate jurisdiction is effective.

(3) The Data Protection Commissioner shall monitor the circumstances applicable to data that has been transferred outside the Republic under subsection (1)(a)(ii) in order to review decisions made under this Act.

(4) Despite subsection (2), personal data may be transferred outside the Republic—

(a) in case of an emergency, to a particular person or entity engaged in the provision of health services or emergency services;

(b) where the data subject has explicitly consented to that transfer of sensitive personal data; and

(c) to a particular international organisation or country which complies with subsection (l)(a)(ii), where the Data Protection Commissioner is satisfied that the transfer or class of

transfers is necessary for any class of data controllers or data subjects and does not hamper the effective enforcement of this Act.

(5) The Data Protection Commissioner shall approve standard contracts or intra-group schemes under subsection (l)(a) where contracts or schemes effectively protect the rights of data subjects under this Act, including in relation with further transfers from the transferees of personal data under this subsection to any other person or entity.

(6) Where a data controller seeks to transfer personal data subject to a standard contract or intragroup scheme under subsection (1)(a), it shall certify and periodically report to the Data Protection Commissioner as may be specified, that the transfer is made under a contract that adheres to these standard contractual clauses or intragroup schemes and that it shall bear any liability for the harm caused due to any noncompliance with the standard contractual clauses or intragroup schemes by the transferee.

Part XI – General provisions

72. Right to compensation

A data subject who has suffered damage as a result of an infringement of that data subject's right under this Act, may receive compensation from the data controller or data processor as determined by a court of competent jurisdiction for the damage suffered.

73. Offences

(1) Subject to the other provisions of this Act, a person commits an offence if that person unlawfully discloses sensitive personal data to another person.

(2) A person convicted of an offence under subsection (1) is liable, on conviction, to a fine not exceeding two hundred thousand penalty units, or to imprisonment to a term not exceeding two years, or to both.

74. Power of Data Protection Commissioner to compound certain offences

Where the Data Protection Commissioner is satisfied, after an investigation, or where a person admits that the person has committed an offence under this Act, the Data Protection Commissioner may, compound the offence by collecting from that person a sum of money that the Data Protection Commissioner considers appropriate, but not exceeding fifty percent of the maximum amount of the fine to which that person would have been liable on conviction.

75. Forfeiture

(1) Where there has been a conviction for any of the offences under this Act, the court may pronounce the forfeiture of the medium containing the personal data to which the offence relates or make any other order as it deems fit.

(2) A court may order forfeiture or deletion where the medium containing the personal data does not belong to the person convicted.

(3) A court may, on conviction for an offence under this Act, impose a prohibition to manage any processing of personal data, directly or through an intermediary, for a period that the court determines.

76. Offence by principal officer shareholder or partner of body corporate or unincorporate body

Where an offence under this Act is committed by a body corporate or unincorporate body, with the knowledge, consent or connivance of the director, manager, shareholder or partner, of that body

corporate or unincorporate body, that director, manager, shareholder or partner of the body corporate or unincorporate body commits an offence and is liable, on conviction, to the penalty specified for that offence.

77. General penalty

A person who commits an offence under this Act for which a specified penalty is not provided, is liable, on conviction, to a fine not exceeding three hundred thousand penalty units or to imprisonment for a term not exceeding three years, or to both.

78. Code of conduct

(1) The Data Protection Commissioner may prepare a code of conduct for data controllers, data processors and data auditors.

(2) A code of conduct under subsection (1) shall be binding on data controllers and data processors and shall include—

(a) the provision of information to data subjects regarding confidentiality;

(b) the advertising or representation of services;

(c) fair, accessible format and transparent processing of personal data for all data subjects; and

(d) any other matter relating to the processing of personal data under this Act.

(3) The Data Protection Commissioner shall publish the code of conduct in a *Gazette* or website of general circulation in the Republic for public information.

(4) A code of conduct published under subsection (3), shall be effective from the date of its publication.

(5) A person who contravenes the code of conduct under subsection (1) commits an offence and is liable, on conviction, to a fine not exceeding two hundred thousand penalty units or to imprisonment for a term not exceeding two years, or to both.

79. Guidelines

(1) The Data Protection Commissioner may issue guidelines that are necessary for the better carrying out of the provisions of this Act.

(2) The Data Protection Commissioner shall publish all the guidelines issued under this Act in a daily newspaper of general circulation, and the guidelines shall not take effect until they are so published.

(3) The guidelines issued under subsection (1) shall be binding on all persons regulated under this Act.

(4) A person who contravenes the guidelines under subsection (1), commits an offence and is liable on conviction, to a fine not exceeding two hundred thousand penalty units or to imprisonment for a term not exceeding two years or to both.

80. Register

(1) The Data Protection Commissioner shall keep and maintain a Register in which the Data Protection Commissioner shall keep information that it may determine.

(2) The Register under subsection (1), shall be kept at a place that the Data Protection Commissioner may determine, and shall be open to inspection by the public during normal working hours on payment of a prescribed fee.

81. Auditing of data controller

(1) The Data Protection Commissioner or an independent data auditor licensed by the Data Protection Commissioner under this Act shall, unless otherwise provided under this Act, audit the policies of a data controller and the conduct of processing of personal data annually.

(2) Where a data controller has been authorised to store data on a server or data centre located outside the Republic, the cost of auditing the server or data controller shall be borne by the data controller.

82. Regulations

(1) The Minister may, by statutory instrument make regulations for the better carrying out of the provisions of this Act.

(2) Without limiting the generality of subsection (1), the regulations may make provision for—

(a) limitation of obligations and rights where that limitation is necessary to preserve

(i) state security;

(ii) defence;

(iii) public safety including the economic wellbeing or interest of the State when the processing operation relates to State security matters; and

(iv) the prevention, investigation, and proof of criminal offence;

(b) the notification of security breaches;

(c) licensing of data auditors;

(d) processing of genetic, biometric and health data;

(e) processing of unique patient identifier;

(f) personal data of children;

(g) data retention; and

(h) registration of data controllers and data processors.

