

General Scheme

Communications (Retention of Data) Bill 2017

Arrangement of Heads

1. Interpretation
2. Non-Application of Act
3. Obligation to retain subscriber data
4. Disclosure request for subscriber data
5. Application for Ministerial Order to retain traffic and location data
6. Ministerial Order to retain traffic and location data
7. Obligation to retain traffic and location data
8. Application for authorisation (judicial) to disclose traffic and location data
9. Appointment of panel of judges / authorisation (judicial) to disclose traffic and location data
10. Variation of Authorisation (judicial) to disclose traffic and location data
11. Approval to make a disclosure request in cases of urgency
12. Data security
13. Destruction arrangements
14. Access to data
15. Notification post facto
16. Designated Officers
17. Penalties
18. Review of operation of Act by designated judge
19. Retention of materials relating to applications, orders, authorisations and approvals.
20. Restriction of disclosure of existence of orders, authorisation, approvals and other documents
21. Compilation of statistics
22. Complaints procedure
23. Regulations
24. Repeal
25. Short Title and commencement
26. Schedule

Head 1 Interpretation

Provide that:

(1). In this Bill-

“Act of 1993” means the Interception of Postal Packets and Telecommunications Messages (Regulation) Act 1993;

“authorisation” means an authorisation under Head 9 to make a disclosure request to a service provider to disclose traffic and location data;

“Competition and Consumer Protection Commission” has the meaning assigned to it by section 9 of the Competition and Consumer Protection Act 2014;

“competition offence” means an offence under section 6 of the Competition Act 2002, that is an offence involving an agreement, decision or concerted practice to which subsection (2) of that section applies;

“subscriber data” means data which identifies a subscriber;

“traffic and location data” means –

- (a) data processed for the purpose of sending, receiving or storing a communication by means of an electronic communications network or for the purpose of charging a subscriber or user in respect of a communication so sent, received or stored, or
- (b) data processed by means of an electronic communications network that identifies the geographic location of the device or equipment used by a user when availing of a publicly available electronic communications service;

“designated judge” means the judge of the High Court designated by the President of the High Court under section 8 of the Act of 1993;

“designated officer” means an officer designated under Head 16 of this Bill;

“disclosure request” means a request to a service provider under Head 4, 9 or 11 for the disclosure of data retained in accordance with this Bill;

“Garda Commissioner “ means the Commissioner of the Garda Síochána;

“Minister” means the Minister for Justice and Equality;

“missing person” means a person who, whether before or after the commencement of this section, is observed to be missing from his or her normal patterns of life, in relation to whom those persons who are likely to have heard from the person are

unaware of the whereabouts of the person and that the circumstances of the person being missing raises concern for his or her safety and well-being;

“processing” has the same meaning as in the Data Protection Act 1988;

‘Referee’ means the holder of the office of Complaints Referee under section 9 of the Act of 1993;

“revenue offence” means an offence under any of the following provisions that is a serious offence:

- (a) Section 1078 of the Taxes Consolidation Act 1997;
- (b) Section 102 of the Finance Act 1999;
- (c) Section 119 of the Finance Act 2001;
- (d) Section 79 (inserted by section 62 of the Finance Act 2005) of the Finance Act 2003;
- (e) Section 78 of the Finance Act 2005;

“serious offence” means an offence punishable by imprisonment for a term of 5 years or more or an offence listed in Schedule 1;

“service provider” means a person who is engaged in the provision of a publicly available electronic communications service or a public communications network by means of fixed line or mobile telephones or the internet;

“superior officer” means –

- (a) in the case of the Garda Síochána, a member of the Garda Síochána not below the rank of Chief Superintendent;
- (b) in the case of the Defence Forces, a member of the Defence Forces not below the rank of Brigadier General;
- (c) in the case of the Revenue Commissioners, an officer of the Revenue Commissioners not below the grade of Assistant Secretary;
- (d) in the case of the Garda Síochána Ombudsman Commission, a member of the Garda Síochána Ombudsman Commission;
- (e) in the case of the Department of Jobs, Enterprise and Innovation, an official of the Department not below the grade of Assistant Secretary;

Head 2 Non-application of Act

Provide that:

2. (1) This Act does not apply to the content of communications transmitted by means of fixed network telephony, mobile telephony, Internet access, internet e-mail or Internet telephony.

Note

This Head makes it clear that the Act does not apply to the content of communications transmitted.

Head 3 Obligation to Retain Subscriber Data

Provide that:

3. (1) A service provider shall retain all subscriber data for a period of 12 months –

(2) The period of retention shall commence –

(a) in the case of data retained under the Communications (Retention of Data) Act 2011 Act, from the date of commencement of this Bill where the date on which the data were first processed is on or after the date which is 12 months prior to the date of commencement of this Bill,

(b) in any other case, on the date on or after the date of commencement of this Bill on which the data were first processed.

(3) Data retained in accordance with subsection (1) shall be retained in such a way that they may be disclosed without undue delay pursuant to a disclosure request.

Note

This Head provides for the retention of subscriber data - subscriber data processed after commencement of the Bill will be retained for 12 months from the date on which it is first processed and, by way of a transitional provision, subscriber data first processed in the 12 months prior to commencement of the Bill will be retained for 12 months from the date of commencement of the Bill.

Head 4 Disclosure request for subscriber data

Provide that:

- (1) A member of the Garda Síochána designated under Head 16 may request a service provider to disclose subscriber data retained by the service provider in accordance with Head 3 where he or she has reasonable grounds for believing that the data which are the subject of the application –
 - (a) relate to a person who is suspected of being or having been involved in the commission of a serious offence, and are necessary for the prevention, detection, investigation or prosecution of that offence; or
 - (b) while not directly related to a person who is suspected of being or having been involved in the commission of the offence, are nevertheless likely to assist in the prevention, detection, investigation or prosecution of that offence.

- (2) A member of the Garda Síochána designated under Head 16 may request a service provider to disclose subscriber data retained by the service provider in accordance with Head 3 where he or she has reasonable grounds for believing that the data which are the subject of the application -
 - (a) relate to a person who is suspected of posing an existing and serious threat to the security of the State, and are necessary for the protection of the State against that threat; or
 - (b) while not directly related to a person who is suspected of posing an existing and serious threat to the security of the State, are nevertheless likely to assist in protecting the State against the threat posed by that person.

- (3) A member of the Garda Síochána designated under Head 16 may request a service provider to disclose subscriber data retained by the service provider in accordance with Head 3 where he or she has reasonable grounds for believing that there is a serious and immediate risk to the health or safety of a person and that the data which are the subject of the application may assist efforts by the Garda Síochána to eliminate or mitigate that risk; where the data are required in the investigation of a missing person or where the data is required for the purpose of assisting the Coroner in the performance of his functions.

- (4) An officer of the Defence Forces designated under Head 16 may request a service provider to disclose subscriber data retained by the service provider in accordance with Head 3 where he or she has reasonable grounds for believing that the data which are the subject of the application –
 - (a) relate to a person who is suspected of posing an existing and serious threat to the security of the State, and are necessary for the protection of the State against that threat; or
 - (b) while not directly related to a person who is suspected of posing an existing and serious threat to the security of the State, are

nevertheless likely to assist in protecting the State from the threat posed by that person.

- (5) An officer of the Revenue Commissioners designated under Head 16 may request a service provider to disclose subscriber data retained by the service provider in accordance with Head 3 where he or she has reasonable grounds for believing that the data which are the subject of the application –
 - (a) relate to a person who is suspected of being or having been involved in the commission of a revenue offence, and are necessary for the prevention, detection, investigation or prosecution of that offence; or
 - (b) while not directly related to a person who is suspected of being or having been involved in the commission of the offence, are nevertheless likely to assist in the prevention, detection, investigation or prosecution of that offence.

- (6) Where an investigation of a serious offence is being carried out under section 98 or 102 of the Garda Síochána Act 2005, an officer of the Garda Síochána Ombudsman Commission designated under Head 16 may request a service provider to disclose subscriber data retained by the service provider in accordance with Head 3 where he or she has reasonable grounds for believing that the data which are the subject of the application –
 - (a) relate to a person who is suspected of being or having been involved in the commission of the offence, and are necessary for the, investigation or prosecution of the offence; or
 - (b) while not directly related to a person who is suspected of being or having been involved in the commission of the offence, are nevertheless likely to assist in the investigation or prosecution of the offence.

- (7) Where the Competition and Consumer Protection Commission are engaged in the prevention, detection, investigation or prosecution of a competition offence, a member of the Commission designated under Head 16 may request a service provider to disclose subscriber data retained by the service provider in accordance with Head 3 where he or she has reasonable grounds for believing that the data which are the subject of the application –
 - (a) relate to a person who is suspected of being or having been involved in the commission of the offence; or
 - (b) while not directly related to a person who is suspected of being or having been involved in the commission of the offence, may nevertheless assist in the prevention, detection, investigation or prosecution of that offence.

- (8) A service provider shall comply with a disclosure request made to the service provider under this Head.

Note

This Head provides for the making of disclosure requests for subscriber data by the competent authorities and sets out the criteria to be considered in the making of such a request.

Head 5 Application for Ministerial Order for the retention of traffic and location data

Provide that:

(1) The Garda Commissioner may make an application to the Minister for the making of an order under Head 6 for the retention of –

(a) a category or specified categories of traffic and location data;
or

(b) traffic and location data in respect of a specified person;

where it is the assessment of the Garda Commissioner that such data is likely to assist in the prevention, detection, investigation or prosecution of serious offences, or the safeguarding of the security of the State.

(2) The Chief of Staff of the Defence Forces may make an application to the Minister for the making of an order under Head 6 for the retention of –

(a) a category or specified categories of traffic and location data;
or

(b) traffic and location data in respect of a specified person;

where it is the assessment of the Chief of Staff of the Defence Forces that such data is likely to assist in the safeguarding of the security of the State.

(3) The Chairman of the Revenue Commissioners may make an application to the Minister for the making of an order under Head 6 for the retention of –

(a) a category or specified categories of traffic and location data;
or

(b) traffic and location data in respect of a specified person;

where it is the assessment of the Chairman of the Revenue Commissioners that such data is likely to assist in the prevention, detection, investigation or prosecution of revenue offences.

(4) A member of the Garda Síochána Ombudsman Commission may make an application to the Minister for the making of an order under Head 6 for the retention of –

(a) a category or specified categories of traffic and location data;
or

(b) traffic and location data in respect of a specified person;

where the investigation of serious offences is being carried out under section 98 or 102 of the Garda Síochána Act 2005 and it is the assessment of the member of the Garda Síochána Ombudsman Commission that such data is likely to assist in the investigation or prosecution of serious offences.

(5) The Chairperson of the Competition and Consumer Protection Commission may make an application to the Minister for the making of an order under Head 6 for the retention of –

(a) a category or specified categories of traffic and location data;
or

(b) traffic and location data in respect of a specified person;

where it is the assessment of the Chairperson of the Competition and Consumer Protection Commission that such data is likely to assist in the prevention, detection, investigation or prosecution of competition offences.

(6) An application under subsection (1), (2), (3), (4) or (5) shall be in writing, in such form as the Minister may prescribe, and shall set out the grounds for the assessment made.

(7) Where the Garda Commissioner, the Chief of Staff of the Defence Forces, the Chairman of the Revenue Commissioners, a member of the Garda Síochána Ombudsman Commission or the Chairperson of the Competition and Consumer Protection Commission, as may be appropriate, considers that the retention of data to which an order under Head 6 of this Bill relates are no longer required, then, without delay he or she shall inform the Minister.

Note

This Head provides for an application to be made, for a Ministerial order to retain traffic and location data, by the Garda Commissioner, the Chief of Staff of the Defence Forces, the Chairman of the Revenue Commissioners, a member of the Garda Síochána Ombudsman Commission or the Chairperson of the Competition and Consumer Protection Commission where it is considered that such data is necessary for the investigation of serious offences or the safeguarding of the security of the State.

Head 6 Ministerial order to retain traffic and location data

Provide that:

(1) Where the Minister receives an application under Head 5, he or she may make an order requiring a service provider to retain –

- (a) a category or specified categories of traffic and location data; or
- (b) traffic and location data in respect of a specified person;

as the case may be, for a specified period which shall not exceed 12 months.

(2) The Minister may renew, vary or revoke an order made under subsection (1), and shall revoke such an order if at any time he or she is no longer satisfied that the requirements of subsection (3) are met.

(3) The Minister shall not make an order under subsection (1) unless he or she is satisfied that the retention of the data to which the order relates -

- (a) is likely to assist in the prevention, detection, investigation or prosecution of serious offences or the safeguarding of the security of the State, and
- (b) is in all the circumstances proportionate;

and that there are no alternative less intrusive means which would be likely to assist as effectively in the prevention, detection, investigation or prosecution of serious offences, or in the safeguarding of the security of the State.

Note

This Head provides that the Minister may make an order for the retention of (a) a category or specified categories of traffic and location data or (b) traffic and location data in respect of a specified individual following a request from the Garda Commissioner, the Chief of Staff of the Defence Forces, the Chairman of the Revenue Commissioners, a member of the Garda Síochána Ombudsman Commission or the Chairperson of the Competition and Consumer Protection Commission under Head 5.

Head 7 Obligation to retain traffic and location data

Provide that:

7. (1) A service provider shall retain traffic and location data in accordance with an order made under Head 6 for a period of 12 months.

(2) The periods of retention referred to in subsection (1) shall commence –

(a) in the case of traffic and location data retained under the Communications (Retention of Data) Act 2011, from the date of commencement of this Bill where the date on which the data were first processed is on or after the date which is 12 months prior to the date of commencement of this Bill,

(b) in any other case, on the date on or after the commencement of this Bill on which the data were first so processed.

(3) Data retained in accordance with subsection (1) shall be retained in such a way that they may be disclosed without undue delay pursuant to a disclosure request.

Note

This Head provides that traffic and location data processed after commencement of the Bill will be retained for 12 months from the date on which it is first processed and that, by way of a transitional provision, traffic and location data first processed in the 12 months prior to commencement of the Bill can be retained for 12 months from the date of commencement of the Bill.

Head 8 Application for authorisation to disclose traffic and location data

Provide that:

- (1) Subject to subsection (8), a member of the Garda Síochána designated under Head 16 may apply to an authorising judge for an authorisation where he or she has reasonable grounds for believing that the data which are the subject of the application –
 - (a) relate to a person who is suspected of being or having been involved in the commission of a serious offence, and are necessary for the prevention, detection, investigation or prosecution of that offence; or
 - (b) while not directly related to a person who is suspected of being or having been involved in the commission of the offence, are nevertheless likely to assist in the prevention, detection, investigation or prosecution of that offence.

- (2) Subject to subsection (8), a member of the Garda Síochána designated under Head 16 may apply to an authorising judge for an authorisation where he or she has reasonable grounds for believing that the data which are the subject of the application -
 - (a) relate to a person who is suspected of posing an existing and serious threat to the security of the State, and are necessary for the protection of the State against that threat; or
 - (b) while not directly related to a person who is suspected of posing an existing and serious threat to the security of the State, are nevertheless likely to assist in protecting the State against the threat posed by that person.

- (3) Subject to subsection (8), a member of the Garda Síochána designated under Head 16 may apply to an authorising judge for an authorisation where he or she has reasonable grounds for believing that there is a serious and immediate risk to the health or safety of a person and that the data which are the subject of the application may assist efforts by the Garda Síochána to eliminate or mitigate that risk; where the data are required in the investigation of a missing person or where the data is required for the purpose of assisting the Coroner in the performance of his functions.

- (4) Subject to subsection (8), an officer of the Defence Forces designated under Head 16 may apply to an authorising judge for an authorisation where he or she has reasonable grounds for believing that the data which are the subject of the application -
 - (a) relate to a person who is suspected of posing an existing and serious threat to the security of the State, and are necessary for the protection of the State against that threat; or

- (b) while not directly related to a person who is suspected of posing an existing and serious threat to the security of the State, are nevertheless likely to assist in protecting the State from the threat posed by that person.

- (5) Subject to subsection (8), an officer of the Revenue Commissioners designated under Head 16 may apply to an authorising judge for an authorisation where he or she has reasonable grounds for believing that the data which are the subject of the application –
 - (a) relate to a person who is suspected of being or having been involved in the commission of a revenue offence, and are necessary for the prevention, detection, investigation or prosecution of that offence; or
 - (b) while not directly related to a person who is suspected of being or having been involved in the commission of the offence, are nevertheless likely to assist in the prevention, detection, investigation or prosecution of that offence.

- (6) Subject to subsection (8), where an investigation of a serious offence is being carried out under section 98 or 102 of the Garda Síochána Act 2005, an officer of the Garda Síochána Ombudsman Commission designated under Head 16 may apply to an authorising judge for an authorisation where he or she has reasonable grounds for believing that the data which are the subject of the application –
 - (a) relate to a person who is suspected of being or having been involved in the commission of the offence, and are necessary for the investigation or prosecution of the offence; or
 - (b) while not directly related to a person who is suspected of being or having been involved in the commission of the offence, are nevertheless likely to assist in the investigation or prosecution of the offence.

- (7) Subject to subsection (8), where the Competition and Consumer Protection Commission are engaged in the prevention, detection, investigation or prosecution of a competition offence, a member of the Commission designated under Head 16 may apply to an authorising judge for an authorisation where he or she has reasonable grounds for believing that the data which are the subject of the application –
 - (a) relate to a person who is suspected of being or having been involved in the commission of the offence; or
 - (b) while not directly related to a person who is suspected of being or having been involved in the commission of the offence, may nevertheless assist in the prevention, detection, investigation or prosecution of that offence.

- (8) An application shall not be made under subsections (1), (2), (3), (4), (5), (6), or (7) unless the person making it is satisfied that the disclosure of data sought to be authorised is –
- (a) the least intrusive means available, having regard to the objectives for which it is being sought and other relevant considerations;
 - (b) proportionate to its objectives, having regard to all the circumstances, including its likely impact on the rights of any person; and
 - (c) is of a scale that is reasonably required to achieve the objectives for which it is being sought.
- (9) An application under this section for an authorisation shall be in writing, in such form as the Minister may prescribe, and shall include –
- (a) the particulars of the offence or the threat to the security of the State in respect of which the authorisation is sought;
 - (b) the particulars of the data sought to be disclosed;
 - (c) the period of time in respect of which the data is sought to be disclosed;
 - (d) the relevance of the data sought to be disclosed to the prevention, detection, investigation or prosecution of the offence concerned, or to the protection of the State from threat, as the case may be, and the use to which the data will be put; and
 - (e) a statement that the person making the application is satisfied as to the matters in subsections (1) to (8).
- (10) Where the Garda Commissioner, the Chief of Staff of the Defence Forces, the Chairman of the Revenue Commissioners, a member of the Garda Síochána Ombudsman Commission or the Chairperson of the Competition and Consumer Protection Commission, as may be appropriate, considers that the retention of data, to which an authorisation issued under Head 9 relates, is no longer required, then, without delay he or she shall inform the authorising judge.

Note

This Head sets out the reasoned and objective criteria to be considered by the competent authorities when making an application for a judicial authorisation to make a disclosure request.

Head 9 Appointment of panel of judges / judicial authorisation to disclose traffic and location data

Provide that:

9.(1) After consulting with the Minister, the President of the District Court shall designate a number of judges of the District Court to undertake (while serving as such judges) the duties specified in this section and, where a District Court judge accepts the invitation, the Government shall designate such judge for the purposes of the Bill.

(2) A judge designated under this Head (referred to in this Bill as an “authorising judge”) shall have the duty of considering applications for authorisations to disclose traffic and location data made in accordance with Head 8 and of issuing such authorisations in accordance with this Head.

(3) An application for an authorisation under Head 8 or for a variation of an authorisation under Head 10 –

(a) shall be made *ex parte* and shall be heard otherwise than in public, and

(b) shall be made to an authorising judge.

(4) An authorising judge shall issue such authorisation as he or she considers reasonable, if satisfied by information on oath of the designated officer concerned that –

(a) the requirements specified in subsection (1), (2), (3), (4), (5), (6) or (7) as the case may be, of Head 8 are fulfilled, and

(b) to do so is justified, having regard to the matters referred to in subsection (8) of Head 8 and all other relevant circumstances.

(5) An authorisation may impose such conditions in respect of the disclosure request as an authorising judge considers appropriate.

(6) An authorisation shall be in writing, in such form as the Minister may prescribe, and shall specify –

(a) the service provider or service providers to which the request is to be made;

- (b) particulars of the data that are authorised to be disclosed;
- (c) the name of the designated officer to whom the authorisation is issued;
- (d) the conditions (if any) subject to which the authorisation is issued;
- (e) the date of expiry of the authorisation.

(7) An authorisation shall expire on the day fixed by an authorising judge that he or she considers reasonable in the circumstances and that is not later than 1 week from the day on which it is issued.

(8) Subject to any conditions imposed by an authorising judge under subsection (5), an authorisation shall have effect both within the District Court district to which the authorising judge is assigned and in any other part of the State.

(9) An authorisation shall authorise the designated officer named in it to make a disclosure request to the service provider or service providers named in it.

(10) A designated officer shall make a disclosure request only in accordance with a valid authorisation issued in accordance with this Head.

(11) A service provider shall comply with a disclosure request made in accordance with this Head.

Note

This Head provides for the designation of District Court judges as “authorising judges” for the purposes of the Bill and sets out the procedures for issuing a judicial authorisation to disclose traffic and location data.

Head 10 Variation/Revocation of judicial authorisation to disclose traffic and location data

Provide that:

10. (1) An authorising judge may, on application in that behalf by an officer designated under Head 16 to whom an authorisation was issued, if satisfied by information on oath of that designated officer justifying the variation of the authorisation, vary the authorisation.

(2) An authorising judge may, on being informed in accordance with subsection (10) of Head 8 that an authorisation issued under Head 9 is no longer required, revoke the authorisation.

Note

This Head provides for the variation or revocation of an authorisation issued under Head 9.

Head 11 Approval to make a disclosure request in cases of urgency

Provide that:

11. (1) An officer designated under Head 16 may make a disclosure request without authorisation where the disclosure request has been approved by a superior officer in accordance with this Head.

(2) A designated officer referred to in subsection (1) may apply to a superior officer for the grant of an approval to make a disclosure request where he or she has reasonable grounds for believing that the requirements specified in subsection (1), (2), (3), (4), (5), (6) or (7) as the case may be, of Head 8 are fulfilled, and to do so is justified, having regard to the matters referred to in subsection (8) of Head 8 and all other relevant circumstances but that, before an authorisation could be issued –

- (a) data in relation to the commission of a serious offence is likely to be destroyed, lost or otherwise become unavailable,
- (b) there is serious and immediate risk to the health or safety of an individual,
- (c) the security of the State would be likely to be compromised.

(3) A superior officer to whom an application under subsection (2) is made shall approve the request for disclosure, having regard to the information in the application, if he or she is satisfied that there are reasonable grounds for believing that an authorisation would be issued under Head 9 but that one or more of the conditions of urgency specified in subsection (2) apply.

(4) An approval may be granted subject to such conditions as the superior officer considers appropriate.

(5) An approval granted under this Head shall permit the designated officer named in it to make a disclosure request to the service provider or service providers named in it.

(6) A designated officer shall make a disclosure request only in accordance with a valid approval granted in accordance with this Head.

(7) A service provider shall comply with a disclosure request made in accordance with this Head.

(8) A superior officer who approves a disclosure request under this Head shall, as soon as practicable and, in any case, not later than 8 hours after the request has been approved, prepare a written record of the approval of the disclosure request.

(9) A written record of approval shall be in such form as the Minister may prescribe by regulations.

(10) The superior officer who granted the approval may vary that approval or any condition attached to it.

(11) A superior officer who approves a request for disclosure under this Head shall make a report as soon as possible and, in any case, not later than 7 days from when the approval was granted specifying the grounds on which the approval was granted and including a copy of the written record of approval.

(12) A report under subsection (11) shall be made to –

(a) in the case of a member of the Garda Síochána, a member of the Garda Síochána of the rank of Assistant Commissioner,

(b) in the case of an officer of the Defence Force, a general officer within the meaning of section 2(b) of the Defence (Amendment) Act 1979) of the Defence Act 1954,

(c) in the case of the Garda Síochána Ombudsman Commission, a member of the Garda Síochána Ombudsman Commission,

(d) in the case of an officer of the Revenue Commissioners, an officer of the Revenue Commissioners of the rank of Assistant Secretary, and

(e) in the case of a member of the Competition and Consumer Protection Commission, an official of the Department of Jobs, Enterprise and Innovation of the rank of Assistant Secretary.

Note

This Head provides for approvals for disclosure requests to be granted by a superior officer in cases of exceptional urgency.

Head 12

Data Security

Provide that:

12. (1) A service provider who retains data in accordance with Head 3 and Head 7 shall take the following security measures in relation to the retained data:

(a) the data shall be of the same quality and subject to the same security and protection as those data relating to the publicly available electronic communications service or to the public communications network, as the case may be;

(b) the data shall be subject to appropriate technical and organisational measures to protect the data against accidental or unlawful destruction, accidental loss or alteration, or unauthorised or unlawful storage, processing, access or disclosure;

(c) the data shall be subject to appropriate technical and organisational measures to ensure that they can be accessed by authorised personnel only;

(d) the data shall be retained within the EU.

Note

This Head, which is based on section 4 of the Communications (Retention of Data) Act 2011, places an onus on service providers to provide sufficient security measures to protect retained data. The data is to be retained in the EU.

Head 13 Destruction arrangements

Provide that:

13. (1) Data which are retained by a service provider in accordance with Head 3 or Head 7, except those that have been requested to be disclosed in accordance with a disclosure request under Head 4, Head 9 or Head 11, shall be irreversibly destroyed by the service provider not later than the expiration of a period of one month from the date on which the period of retention for that data ends.

(2) Data which are disclosed in accordance with Head 4, Head 9 or Head 11 shall be irreversibly destroyed by the Garda Commissioner, the Chief of Staff of the Defence Forces, the Chairman of the Revenue Commissioners, a member of the Garda Síochána Ombudsman Commission or the Chairperson of the Competition and Consumer Protection Commission, as may be appropriate, in any of the following circumstances, not later than the expiration of a period of one month from the date on which such circumstances apply –

(a) where proceedings for the offence in relation to which the data were retained and disclosed –

(i) are not instituted against the person within the period of 12 months from the date on which the data were first disclosed, or

(ii) have been instituted and are final.

(3) Where data are to be irreversibly destroyed in accordance with subsection (2) of this Head, the Garda Commissioner; the Chief of Staff of the Defence Forces; the Chairman of the Revenue Commissioners; a member of the Garda Síochána Ombudsman Commission or the Chairperson of the Competition and Consumer Protection Commission, as appropriate, shall inform the service provider who disclosed the data in accordance with Head 4, Head 9 or Head 11, in writing, that the data are to be irreversibly destroyed and the data shall be irreversibly destroyed by the service provider not later than one month from the date on which the service provider is so informed.

(3) The Minister, the Minister for Defence, the Minister for Finance and the Minister for Jobs, Enterprise and Innovation may make regulations prescribing the procedures and arrangements for the destruction of data retained and disclosed under this Act.

Note

This Head provides for destruction arrangements in relation to data retained by service providers and by competent authorities in respect of data disclosed to them.

Head 14 Access to Data

Provide that:

14. (1) Without prejudice to any other right to access data provided for in accordance with law, a service provider shall not access data retained in accordance with Head 3 or Head 7 except—

- (a) in the course of, and to the extent required by, his or her operating duties,
- (b) for the purpose of complying with a disclosure request,
- (c) in accordance with a court order, or
- (d) as may otherwise be authorised by law.

(2.) Where all or part of the period for which data is to be retained in accordance with Head 3 or Head 7 (obligation to retain) coincides with the period during which any of the data specified may, in accordance with law, be processed for purposes other than those specified, nothing in Heads 9 or 11 (disclosure request) shall prevent those data from being processed for those other purposes.

Note

This Head provides for protection against improper access of the retained data (subhead (1)) and that a disclosure request will not prevent the processing of retained data for other purposes in accordance with law (subhead (2)).

Head 15 Notification Post Facto

Provide that:

15. (1) Where a person has been the subject of a disclosure request or other persons' interests are materially affected by such disclosure request, the Garda Commissioner, the Chief of Staff of the Defence Forces, the Chairman of the Revenue Commissioners, a member of the Garda Síochána Ombudsman Commission or the Chairperson of the Competition and Consumer Protection Commission shall cause the person or persons to be informed by notice in writing of the existence of an authorisation issued or approval granted under Heads 9 or 11 of the Bill.

(2) The Minister may make regulations respecting the disclosure or non-disclosure, to the person who was its subject or other persons whose interests are materially affected by it, of the existence of an authorisation issued or approval granted under Heads 9 or 11, provided that any disclosure authorised by such regulations is—

(a) consistent with the purposes for which the authorisation or approval concerned was issued or granted;

(b) consistent with the protection of persons' privacy and other rights, the aims of the prevention and detection of the commission of serious offences and the security of the State;

(c) unlikely to jeopardise the investigation of such offences being undertaken or to be undertaken in the future, and

(d) unlikely to result in risk to the life or safety of a person or persons.

(3) Any Regulation made under subsection (2) may—

(a) provide that the Director of Public Prosecutions shall assess whether it is in order, in any particular case of disclosure, to inform the individual affected;

(b) require consultation by the Minister, in any particular case of disclosure, with such classes of persons as may be prescribed;

(c) prescribe categories of persons (other than the subjects of the authorisations or approvals) whose interests are materially affected by authorisations or approvals, to whom disclosure is to be made; and

(d) permit the imposition of terms and conditions limiting the extent or detail of disclosure as necessary, having regard to the matters referred to in subsection (2).

Note

This Head provides for the notification of a person who has been the subject of a disclosure request or other persons whose interests have been materially affected by the disclosure request and for the making of regulations outlining the procedures for notification of the individual whose data have been accessed.

Head 16 Designated Officers

Provide that:

16. (1) The Garda Commissioner may designate a member of the Garda Síochána not below the rank of Chief Superintendent as a designated officer for the purposes of this Bill.

(2) The Chief of Staff of the Defence Forces may designate an officer of the Defence Force not below the rank of Colonel as a designated officer for the purposes of this Bill.

(3) The Minister for Finance may designate an officer of the Revenue Commissioners not below the grade of Principal Officer as a designated officer for the purposes of this Bill.

(4) The Garda Síochána Ombudsman Commission may designate an officer of the Garda Síochána Ombudsman Commission as a designated officer for the purposes of this Bill.

(5) The Minister for Jobs, Enterprise and Innovation may designate a member of the Competition and Consumer Protection Commission as a designated officer for the purposes of this Bill.

Note

This Head provides for the designation of senior officers of the competent authorities concerned as designated officers for the purposes of the Bill.

Head 17 Penalties (for service providers for failing to comply with obligations to retain/disclose)

Provide that:

17. (1) A person who fails to comply with a requirement in relation to the retention of data under Head 3 or Head 7 or to the disclosure of data under Heads 4, 9 or 11 or who accesses data retained in accordance with Head 3 or Head 7 without lawful authority or reasonable excuse shall be liable –

(a) on summary conviction to a class [] fine or imprisonment for a term not exceeding [] months or both, or

(b) on conviction on indictment, to a fine or imprisonment for a term not exceeding [] years or both.

Note

This Head provides for penalties on summary conviction or on conviction on indictment for contravention of the provisions governing data retention under Heads 3 or 7 or disclosure of data under Heads 4, 9 or 11 or access under Head 14.

Head 18 Review of operation of Act by designated judge

Provide that:

18. (1) Section 8 the Act of 1993 is amended by the substitution of the following for subsection (1):

“(1) The President of the High Court shall from time to time after consulting with the Minister invite a person who is a judge of the High Court to undertake (while serving as such a judge) the duties specified in this section and Head 18 of the Communications (Retention of Data) Act 2017 and, if the invitation is accepted, the Government shall designate the judge for the purposes of this Act and the Communications (Retention of Data) Act 2017.

(1A) Subsection (1) does not affect the functions of the Data Protection Commissioner under section 10 of the Data Protection Act 1988 .”.

(2) In addition to the duties assigned under section 8 of the Act of 1993, the designated judge shall—

- (a) keep the operation of the provisions of this Bill under review,
- (b) ascertain whether the Garda Síochána, the Defence Forces the Revenue Commissioners, the Garda Síochána Ombudsman Commission and the Competition and Consumer Protection Commission are complying with its provisions, and
- (c) include, in the report to the Taoiseach under section 8(2) of the Act of 1993, such matters relating to this Bill as the designated judge considers appropriate.

(3) For the purpose of carrying out the duties assigned under this Head, the designated judge—

- (a) may investigate any case in which an authorisation is issued under Head 9 or an approval is granted under Head 11, and
- (b) may access, and has the power to inspect, the authorisations, written records of approval, reports and other relevant documents that the designated judge may request.

(5) The designated judge may, if he or she considers it desirable to do so, communicate with the Taoiseach or Minister concerning authorisations issued or

approvals granted, with the Director of Public Prosecutions concerning notification of individuals whose data have been disclosed, and with the Data Protection Commissioner in connection with the Commissioner's functions under the Data Protection Acts.

Note

This Head provides for a review of the operation of the Bill by the judge designated under the Interception of Postal Packets and Telecommunications Messages (Regulation) Act 1993 to review that Act.

Head 19 Retention of materials relating to applications, orders, authorisations and approvals

Provide that:

19. (1) An application for an order under Head 6, for an authorisation under Head 8 or for an approval under Head 11 and any documents supporting such applications shall be retained until -

(a) the day that is 3 years after the day on which the order, approval or authorisation concerned ceases to be in force, or

(b) the day on which they are no longer required for any prosecution or appeal to which they are relevant,

whichever is later.

Note

This Head provides for the retention of documents relating to the application for an order or for an authorisation or approval for a period of 3 years or until they are no longer required for any prosecution or appeal.

Head 20 Restriction of disclosure of existence of orders, authorisations, approvals and other documents

Provide that:

20. (1) The Garda Commissioner, the Chief of Staff of the Defence Forces, the Chairman of the Revenue Commissioners, a member of the Garda Síochána Ombudsman Commission or the Chairperson of the Competition and Consumer Protection Commission shall ensure that information and documents to which this Bill applies are stored securely and that only persons who he or she authorises for that purpose shall have access to them.

(2) In the interests of protecting the privacy and other rights of persons, preventing the commission of and detecting serious offences and safeguarding the security of the State, the Minister, the Minister for Defence, the Minister for Finance and the Minister for Jobs, Enterprise and Innovation may make regulations prescribing –

(a) the persons or categories of persons who are to have access for the purpose of this Head to information with respect to the existence of orders, authorisations and approvals granted under Head 6, Head 9 or Head 11 and documents referred to in Head 19.

(b) the procedures and arrangements for the secure storage, and the maintenance of the security, of that information and those documents, and

(c) the number of copies that may be made of those documents and the destruction of those copies as soon as possible after they are no longer required under Head 19.

Note

This Head provides for restriction on disclosure of the existence of orders, authorisations, approvals or other documents.

Head 21 Reporting

Provide that:

21. (1) The Garda Commissioner shall prepare and submit a report to the Minister, in respect of data that were the subject of a disclosure request made under Head 4, Head 9 or Head 11, on an annual basis.

(2) The Chief of Staff of the Defence Forces shall prepare and submit a report to the Minister for Defence, in respect of data that were the subject of a disclosure request made under Head 4, Head 9 or Head 11, on an annual basis.

(3) The Chairperson of the Revenue Commissioners shall prepare and submit a report to the Minister for Finance, in respect of data that were the subject of a disclosure request made under Head 4, Head 9 or Head 11, on an annual basis.

(4) A member of the Garda Síochána Ombudsman Commission shall prepare and submit a report to the Minister, in respect of data that were the subject of a disclosure request made under Head 4, Head 9 or Head 11, on an annual basis.

(5) The Chairperson of the Competition and Consumer Protection Commission shall prepare and submit a report to the Minister for Jobs, Innovation and Enterprise, in respect of data that were the subject of a disclosure request made under Head 4, Head 9 or Head 11, on an annual basis.

(6) A report prepared under subsections (1) to (5) of this Head shall be submitted as soon as is practicable after the end of the relevant period.

(7) The report shall include –

(a) the number of times data were disclosed in response to a disclosure request,

(b) the number of times a disclosure request could not be met,

(c) the average period of time between the date on which the retained data were first processed and the disclosure request.

(8) The Minister for Defence, the Minister for Finance and the Minister for Jobs, Enterprise and Innovation, as appropriate, shall review the report submitted under

subsections (2), (3) and (5) of this Head and shall forward it to the Minister, along with any observations which he or she may have in respect of it.

(9) The Minister shall ensure that a copy of the report is laid before each House of the Oireachtas not later than 6 months after it is made.

Note

This Head provides that an annual report on data disclosed under the Bill should be submitted to the relevant Ministers who, in turn, should submit the reports to the Minister who will ensure that the report is laid before the Houses of the Oireachtas.

Head 22 Complaints Procedure

Provide that:

22.(1) A person who believes that he or she might be the subject of an authorisation under Head 9 or an approval under Head 11 may apply to the Referee for an investigation into the matter.

(2) A superior officer who makes a report under section 11(11) or who receives a report under section 11(12) may apply to the Referee for an investigation into a matter if he or she believes that such an investigation would be in the interests of justice.

(3) If an application is made under this Head (other than one that the Referee considers to be frivolous or vexatious), the Referee shall investigate—

(a) whether an authorisation was issued or an approval was granted as alleged in the application, and

(b) if so, whether any provision of Head 4, Head 9 or Head 11 has been contravened in relation to the disclosure request.

(4) If, after investigating the matter, the Referee concludes that a provision of Head 4, Head 9 or Head 11 has been contravened, the Referee shall—

(a) notify the applicant, and any other person whose interests are materially affected by the contravention, in writing of that conclusion, and

(b) make a report of his or her findings to the Taoiseach.

(5) In the circumstances referred to in subsection (4), the Referee may also, if he or she is of opinion that the contravention was material and that to do so would be justified in the circumstances, by order do one or more of the following things:

(a) direct -

(i) the quashing of the authorisation or the reversal of the approval, and

(ii) the destruction of the written record of approval concerned, the report under Head 11(11) and any information or documents obtained as a result of the authorisation or approval.

(b) report the matter and any recommendation under subsection 5(b) to the Garda Commissioner, the Chief of Staff of the Defence Forces, the Chairman of the Revenue Commissioners, a member of the Garda Síochána Ombudsman Commission or the Chairperson of the Competition and Consumer Protection Commission, as may be appropriate.

(c) report the matter and any recommendation under subsection 5(b) to the judge designated under Head 18.

(6) If, after investigating the matter, the Referee concludes that there has not been a contravention, the Referee shall give notice in writing to the applicant stating only that there has been no such contravention.

(7) A decision of the Referee under this Head is final.

(8) For the purpose of an investigation under this Head, the Referee is entitled to access, and has the power to inspect, the authorisations, written records of approval, reports and other relevant documents that the Referee may request.

Note

This Head provides for a complaints procedure where a person believes that data relating to him has been disclosed otherwise than in accordance with the Act.

Head 23

Regulations

Provide that:

23. (1) The Minister, the Minister for Defence, the Minister for Finance and the Minister for Jobs, Enterprise and Innovation may make regulations prescribing any matter or thing which is referred to in this Bill as prescribed or to be prescribed by him or her.

(2) Regulations made under this Head may contain such incidental, supplementary and consequential provisions as appear to the Minister of the Government making them to be necessary or expedient for the purposes of the regulations.

(3) Every regulation made under this Head shall be laid before each House of the Oireachtas as soon as may be after it has been made and, if a resolution annulling the regulation is passed by either such House within the next 21 days on which that House has sat after the regulation is laid before it, the regulation shall be annulled accordingly, but without prejudice to the validity of anything previously done thereunder.

Note

This Head is a standard provision providing for the making of regulations under the Bill.

Head 24 Repeal

Provide that:

24. (1) The Communications (Retention of Data) Act 2011 is repealed.

Note

This Head provides for the repeal of the Communications (Retention of Data) Act 2011.

Head 25 Short Title and commencement

Provide that:

25.(1) This Bill may be cited as the Communications (Retention of Data) Bill 2017.

(2) This Bill shall come into operation on such day or days as may be appointed by order or orders made by the Minister either generally or with reference to a particular purpose or provision and different days may be so appointed for different purposes and different provisions.

Head 26 Schedule 1

Provide that:

A Schedule of Offences deemed to be Serious Offences for the purposes of this Act

SCHEDULE 1

Offences Deemed to be Serious Offences

1. An offence under sections 11 and 12 of the Criminal Assets Bureau Act 1996 .
2. An offence under section 6 of the Criminal Evidence Act 1992 .
3. An offence under section 12 of the Non-Fatal Offences against the Person Act 1997 .
4. An offence under section 1 of the Prevention of Corruption Acts 1889 to 2010

Note

An offence under sections 11 and 12 of the Criminal Assets Bureau Act 1996. These offences relate to the publication of information regarding a current or former member of the Criminal Assets Bureau, information concerning their family or details of their primary residence.

An offence under section 6 of the Criminal Evidence Act 1992. This offence relates to knowingly providing false or incorrect evidence in criminal proceedings.

An offence under section 12 of the Non-Fatal Offences against the Person Act 1997. This offence relates to intentionally or recklessly administering a poisonous substance, capable of rendering a person unconscious or interfering with their bodily functions.

An offence under section 1 of the of the Prevention of Corruption Acts 1889 to 1995. This section relates to a person accepting an inducement to perform a specific act or make a deliberate omission in the performance of their duties.

