Number 3 *of* 2011

COMMUNICATIONS (RETENTION OF DATA) ACT 2011

REVISED

Updated to 1 August 2023

This Revised Act is an administrative consolidation of the *Communications (Retention of Data) Act 2011*. It is prepared by the Law Reform Commission in accordance with its function under the *Law Reform Commission Act 1975* (3/1975) to keep the law under review and to undertake revision and consolidation of statute law.

All Acts up to and including the *Wildlife (Amendment) Act 2023* (25/2023), enacted 20 July 2023, and all statutory instruments up to and including the *Criminal Justice (Miscellaneous Provisions) Act 2023 (Commencement) Order 2023* (S.I. No. 391 of 2023), made 28 July 2023, were considered in the preparation of this Revised Act.

Number 3 *of* 2011

COMMUNICATIONS (RETENTION OF DATA) ACT 2011

REVISED

Updated to 1 August 2023

ARRANGEMENT OF SECTIONS

Section

ACTS REFERRED TO

Criminal Assets Bureau Act 1996	1996, No. 31
Criminal Evidence Act 1992	1992, No. 12
Criminal Justice (Terrorist Offences) Act 2005	2005, No. 2
Customs Consolidation Act 1876	39 & 40, Vict. Ch. 36
Data Protection Act 1988	1988, No. 25
Data Protection Acts 1988 and 2003	
Finance Act 1999	1999, No. 2
Finance Act 2001	2001, No. 7
Finance Act 2003	2003, No. 3
Finance Act 2005	2005, No. 5

Interception of Postal Packets and Telecommunications Messages (Regulation) Act 1993	1993, No. 10
Non-Fatal Offences against the Person Act 1997	1997, No. 26
Prevention of Corruption Acts 1889 to 1995	
Protections for Persons Reporting Child Abuse Act 1998	1998, No. 49
Taxes Consolidation Act 1997	1997, No. 39

Number 3 *of* 2011

COMMUNICATIONS (RETENTION OF DATA) ACT 2011

REVISED

Updated to 1 August 2023

AN ACT TO GIVE EFFECT TO DIRECTIVE NO. 2006/24/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL OF 15 MARCH 2006 [1] ON THE RETENTION OF DATA GENERATED OR PROCESSED IN CONNECTION WITH THE PROVISION OF PUBLICLY AVAILABLE ELECTRONIC COMMUNICATIONS SERVICES OR OF PUBLIC COMMUNICATIONS NETWORKS AND AMENDING DIRECTIVE 2002/58/EC [2], TO PROVIDE FOR THE RETENTION OF AND ACCESS TO CERTAIN DATA FOR THE PURPOSES OF THE PREVENTION OF SERIOUS OFFENCES, THE SAFEGUARDING OF THE SECURITY OF THE STATE AND THE SAVING OF HUMAN LIFE, TO REPEAL PART 7 OF THE CRIMINAL JUSTICE (TERRORIST OFFENCES) ACT 2005, TO AMEND THE INTERCEPTION OF POSTAL PACKETS AND TELECOMMUNICATIONS MESSAGES (REGULATION) ACT 1993 AND TO PROVIDE FOR RELATED MATTERS.

[26*th January*, 2011]

BE IT ENACTED BY THE OIREACHTAS AS FOLLOWS:

Interpretation.

1.— (1) In this Act—

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

F1**[**"authorising judge" means a judge of the District Court designated under *section 12J(1)*;**]**

"cell ID" means the identity of the cell from which a mobile telephony call originated or in which it terminated;

F2**[**"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;**]**

"data" means traffic data or location data and the related data necessary to identify the subscriber or user;

"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;

F1**[**"disclosure requirement" means a requirement made of a service provider under *section 6, 6F, 7C* or *7D*;

"electronic communications network" means transmission systems and, where applicable—

[1] O.J. No. L105, 13.04.2006, p. 54
[2] O.J. No. L201, 31.07.2002, p. 37

(*a*) switching equipment or routing equipment, and

(*b*) other resources,including network elements which are not active, which permit the conveyance of signals by wire, by radio, by optical or by other electromagnetic means, and such conveyance includes the use of—

(i) satellite networks,

(ii) fixed terrestrial networks (both circuit-switched and packet-switched, including internet),

(iii) mobile terrestrial networks,

(iv) electricity cable systems to the extent that they are used for the purpose of transmitting signals,

(v) networks used for either or both radio and television broadcasting, and

(vi) cable television networks,

irrespective of the type of information conveyed;

"electronic communications service" means a service normally provided for remuneration which consists wholly or mainly in the conveyance of signals on electronic communications networks, including telecommunications services, publicly available telephone services and transmission services in networks used for broadcasting, but does not include—

(*a*) services providing, or exercising editorial control over, content transmitted using electronic communications networks and services, and

(*b*) information society services within the meaning of Article 1 (inserted by Directive 98/48/EC of 20 July 1998[1]) of Directive 98/34/EC of 22 June 1998[2] which do not consist wholly or mainly in the conveyance of signals on electronic communications networks;**]**

F3**[**...**]**

"Garda Commissioner" means the Commissioner of the Garda Síochána;

F1**[**"internet source data" means the following data necessary to trace and identify the source of a communication by internet access, internet email or internet telephony:

(*a*) the Internet Protocol (IP) address, whether dynamic or static, allocated by the service provider to the source of a communication;

(*b*) the name and address of the subscriber or registered user to whom an Internet Protocol (IP) address was allocated at the time of the communication;**]**

"Minister" means the Minister for Justice, Equality and Law Reform;

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

"Referee" means the holder of the office of Complaints Referee under the Act of 1993;

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

(*a*) section 186 of the Customs Consolidation Act 1876;

(*b*) section 1078 of the Taxes Consolidation Act 1997;

(*c*) section 102 of the Finance Act 1999;

[1] O.J. No. L 217, 05.08.1998, p.18
[2] O.J. No. L 204, 21.07.1998, p.37

(*d*) section 119 of the Finance Act 2001;

(*e*) section 79 (inserted by section 62 of the Finance Act 2005) of the Finance Act 2003;

(*f*) section 78 of the Finance Act 2005;

F1**[**"Schedule 2 data" means the categories of data specified in *Parts 1* and *2* of *Schedule 2*;**]**

"serious offence" means an offence punishable by imprisonment for a term of 5 years or more, and an offence listed in *Schedule 1* is deemed to be a serious offence;

"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;

F1**[**"superior officer" means—

(*a*) in relation to a member of the Garda Síochána, a member of the Garda Síochána not below the rank of superintendent;

(*b*) in relation to a member of the Permanent Defence Force, a member of the Permanent Defence Force not below the rank of lieutenant colonel;

(*c*) in relation to an officer of the Revenue Commissioners, an officer of the Revenue Commissioners not below the rank of principal officer;**]**

F4**[**(*d*) in relation to an officer of the Competition and Consumer Protection F5**[**Commission**]**, an officer of the Competition and Consumer Protection F5**[**Commission**]** not below the rank of principal officer;**]**

"telephone service" means calls (including voice, voicemail, conference and data calls), supplementary services (including call forwarding and call transfer) and messaging and multimedia services (including short message services, enhanced media services and multi-media services);

"unsuccessful call attempt" means a communication where a telephone call or an Internet telephony call has been successfully connected but not answered or there has been a network management intervention;

F6**[**"user" means a person who is using an electronic communications service or other means of electronic communication, for private or other purposes—

(*a*) whether or not that electronic communications service or other means of electronic communication is publicly available, and

(*b*) whether or not that person has subscribed to the service;**]**

F1**[**"user data" means the following types of data and any other types of data set out in technical specification ETSI TS 103 280 "Lawful Interception (LI): dictionary for common parameters" issued by the European Telecommunications Standards Institute that are relevant to these data:

(*a*) the name of the user;

(*b*) the address of the user;

(*c*) where applicable, the following data in respect of the user:

(i) the mobile telephony number;

(ii) the fixed network telephony number;

(iii) the International Mobile Subscriber Identifier (IMSI);

(iv) the International Mobile Equipment Identity (IMEI);

(v) the Internet Protocol (IP) address, whether dynamic or static, allocated by the internet access service to the communication;

(vi) the user ID;

(vii) the date and time of initial activation of an electronic communications service or other means of communication;

(viii) the date and time of the last outgoing mobile telephony or fixed network telephony communication;**]**

"user ID" means a unique identifier allocated to a person when they subscribe to or register with an Internet access service or Internet communications service.

(2) A word or expression used in this Act and also in Directive 2002/58/EC has the same meaning in this Act as in that Directive.

Non-application of Act.

2.— 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.

F7**[**Obligation to retain data

3.— (1) A service provider shall retain, in accordance with *section 12D*, user data for a period of one year, or such period as may be prescribed in accordance with *subsection (2)*, from the date on which the data were first processed by the service provider concerned.

(2) The Minister may, for the purposes of *subsection (1)*, prescribe such period (which may be less than one year, and which shall not exceed two years) as he or she considers necessary for, and proportionate to, the purposes of—

(*a*) preventing, detecting, investigating or prosecuting offences, including revenue offences and competition offences,

(*b*) achieving the objectives specified in *section 6(1)(b)*.

(3) The Minister may, in prescribing a period under *subsection (2)*, prescribe different periods for different types of data specified in the definition of "user data" in this Act.**]**

F8**[**Obligation to retain Schedule 2 data

3A.— (1) The Minister may, where he or she is satisfied that there exists a serious and genuine, present or foreseeable threat to the security of the State, make, in accordance with this section, an application to a relevant judge for an order under this section.

(2) Before making an application under *subsection (1)*, the Minister shall assess the threat to the security of the State and, in doing so shall have regard to the necessity and proportionality of the retention of *Schedule 2* data pursuant to an order under this section, taking into account the impact of such retention on the fundamental rights of individuals.

(3) An application under *subsection (1)* shall—

(*a*) be made *ex parte*,

(*b*) be upon information on oath specifying the grounds on which the order is sought, which information shall include the assessment under *subsection (2)* concerned,

(*c*) specify the period of time for which retention of Schedule 2 data by service providers is, in the view of the Minister, having regard to his or her

assessment under *subsection (2)*, required for the purposes of safeguarding the security of the State, and

(*d*) be heard otherwise than in public.

(4) A relevant judge, as respects an application under *subsection (1)*, may make an order under *subsection (5)* only if satisfied that the making of such an order is necessary for, and proportionate to, the purposes for which the application was made.

(5) An order under this subsection shall require all service providers to retain *Schedule 2* data, or such *Schedule 2* data as are specified in the order—

(*a*) for a period of 12 months from the date on which the data were first processed by the service provider concerned,

(*b*) in accordance with *section 12D*, and

(*c*) subject to such conditions and directions as the relevant judge may specify in the order.

(6) Where a relevant judge makes an order under *subsection (5)*, the Minister shall, without delay arrange for—

(*a*) the order to be publicised in the national media,

(*b*) the order to be notified, in so far as practicable, to service providers, and

(*c*) a notice of the making of the order to be published in *Iris Oifigiúil*.

(7) A service provider shall comply with an order under *subsection (5)*.

(8) The data to which this section applies include data relating to unsuccessful call attempts that, in the case of data specified in *Part 1* of F9**[***Schedule 2***]**, are stored in the State, or in the case of data specified in *Part 2* of F9**[***Schedule 2***]**, are logged in the State.

(9) An order under this section shall not require a service provider to retain aggregated data, data that have been made anonymous or data relating to unconnected calls.

(10) The President of the High Court shall at the request of the Minister, designate a judge or judges of the High Court to perform the functions of a relevant judge under this section, and a reference in this section to a "relevant judge" shall be construed as a reference to a judge so designated.

(11) In this section, "aggregated data" means data that cannot be related to individual users.**]**

F10**[**Obligation to retain internet source data.

3B.— (1) A service provider shall retain, in accordance with *section 12D*, internet source data for a period of one year, or such period as may be prescribed in accordance with *subsection (2)*, from the date on which the data were first processed by the service provider concerned.

(2) The Minister may, for the purposes of *subsection (1)*, prescribe such period (which may be less than one year, and which shall not exceed two years) as he or she considers necessary for, and proportionate to, the purposes of safeguarding the security of the State or achieving the objectives specified in *section 6C(1)(b)*.**]**

Data security.

4.— (1) A service provider who F11**[**retains or preserves**]** data under F12**[***section 3(1), 3A(5), 3B(1), 7A(11)* or *7B(10)***]** 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;

F12**[**(*d*) the data, except those that have been accessed and preserved, shall be destroyed by the service provider in such manner, and within such period (which shall not exceed 2 years and one month) as may be prescribed.**]**

(2) The Data Protection Commissioner is hereby designated as the national supervisory authority for the purposes of this Act and Directive No. 2006/24/EC of the European Parliament and of the Council.

Access to data.

5.— A service provider shall not access data retained in accordance with *section 3* except—

(*a*) at the request and with the consent of a person to whom the data relate,

(*b*) for the purpose of complying with a F13**[**disclosure requirement**]**,

(*c*) in accordance with a court order, or

(*d*) as may be authorised by the Data Protection Commissioner.

F14**[**Requirement to disclose user data

6.— (1) A member of the Garda Síochána not below the rank of superintendent may require a service provider to disclose to that member user data in the possession or control of the service provider—

(*a*) where the member believes that the data relate to a person whom the member suspects, on reasonable grounds of—

(i) having committed an offence, or

(ii) presenting an actual or potential threat to the security of the State,

or

(*b*) where the member has reasonable grounds for believing that the data are otherwise required for the purpose of—

(i) preventing, detecting, investigating or prosecuting offences,

(ii) safeguarding the security of the State,

(iii) protecting the life or personal safety of a person, in circumstances where the member believes that there is a serious risk to the life or personal safety of the person, or

(iv) determining the whereabouts of a missing person.

(2) A member of the Permanent Defence Force not below the rank of lieutenant colonel may require a service provider to disclose to that member user data in the possession or control of the service provider—

(*a*) where the member believes that the data relate to a person whom the member suspects, on reasonable grounds, of presenting an actual or potential threat to the security of the State, or

(*b*) where the member has reasonable grounds for believing that the data are otherwise required for the purpose of safeguarding the security of the State.

F15**[**(3) An officer of the Revenue Commissioners not below the rank of principal officer may require a service provider to disclose to that officer user data in the possession or control of the service provider—

(*a*) where the F16**[**officer**]** believes that the data relate to a person whom the officer suspects, on reasonable grounds, of having committed a revenue offence, or

(*b*) where the officer has reasonable grounds for believing that the data are otherwise required for the purpose of preventing, detecting, investigating or prosecuting a revenue offence.

(4) An officer of the Competition and Consumer Protection Commission not below the rank of principal officer may require a service provider to disclose to that officer user data in the possession or control of the service provider—

(*a*) where the F16**[**officer**]** believes that the data relate to a person whom the officer suspects, on reasonable grounds, of having committed a competition offence, or

(*b*) where the officer has reasonable grounds for believing that the data are otherwise required for the purpose of preventing, detecting, investigating or prosecuting a competition offence.**]**

(5) Subject to *subsection (6)*, a requirement under this section shall be given to a service provider by notice in writing.

(6) If the member or officer concerned considers that the circumstances that warrant the making of a requirement under this section are of exceptional urgency, he or she may make such a requirement other than in writing.

(7) A member or officer who makes a requirement under this section in accordance with *subsection (6)* shall, not later than 2 days after the making of the requirement, give to the service provider of whom the requirement was made a notice in writing—

(*a*) specifying the requirement, and

(*b*) certifying that the requirement was made other than in writing due to the existence of circumstances of exceptional urgency.

(8) A service provider shall, as soon as practicable after a notice under *subsection (5)* is given to him or her or, where applicable, a requirement is made of him or her under *subsection (6)*, comply with the requirement concerned.**]**

F17**[**Authorisation to require disclosure of *Schedule 2* data

6A.— (1) A member of the Garda Síochána not below the rank of inspector may apply to an authorising judge for an authorisation under this section where the member is of the belief that the *Schedule 2* data in respect of which the application is made—

(*a*) relate to a person whom the member suspects, upon reasonable grounds, of presenting an actual or potential threat to the security of the State, or

(*b*) are otherwise required for the purpose of safeguarding the security of the State.

(2) A member of the Permanent Defence Force not below the rank of commandant may apply to an authorising judge for an authorisation under this section where the

member is of the belief that the *Schedule 2* data in respect of which the application is made—

(*a*) relate to a person whom the member suspects, upon reasonable grounds, of presenting an actual or potential threat to the security of the State, or

(*b*) are otherwise required for the purpose of safeguarding the security of the State.

(3) An application for an authorisation under this section shall—

(*a*) be made *ex parte*,

(*b*) be upon information on oath, specifying the grounds on which the order is sought,

(*c*) specify, by reference to the criteria specified in *subsection (6)*, the terms of the authorisation sought, and

(*d*) be heard otherwise than in public.

(4) An authorising judge, as respects an application for an authorisation under this section, may issue an authorisation only if satisfied that—

(*a*) *paragraph (a)* or *(b)* of *subsection (1)* or, as the case may be, *subsection (2)*, applies in respect of the application, and

(*b*) the issuing of the authorisation is necessary for, and proportionate to, the purposes for which the application is made.

(5) An authorisation under this section shall authorise the applicant concerned, at any time in the period during which the authorisation has effect, to require the service provider specified in the authorisation to disclose to that applicant *Schedule 2* data in the service provider's possession or control—

(*a*) of such class or classes as are specified in the authorisation, and

(*b*) subject to such conditions and directions as may be specified in the authorisation.

(6) For the purposes of *subsection (5)(a)*, an authorising judge may specify a class or classes of *Schedule 2* data by reference to one or more of the following:

(*a*) a particular location or locations;

(*b*) a particular geographical area or areas;

(*c*) a particular period of time;

(*d*) a particular means of communication;

(*e*) a particular person or particular persons;

(*f*) such other matter or feature as the authorising judge considers appropriate.

(7) This section shall apply to *Schedule 2* data irrespective of whether an order under *section 3A* is in effect in relation to such data.**]**

F18**[**Authorisation to require disclosure of *Schedule 2* data in case of urgency

6B.— (1) Subject to *subsection (13)*, a member of the Garda Síochána not below the rank of inspector may apply to a superior officer for an authorisation under this section where the member believes on reasonable grounds that—

(*a*) *paragraph (a)* or *(b)* of *section 6A(1)* applies to the *Schedule 2* data in respect of which the application is made, and

(*b*) it is likely that, before the *Schedule 2* data could be obtained pursuant to an authorisation under *section 6A*—

(i) the data would be wholly or partly destroyed or otherwise rendered unavailable, or

(ii) the security of the State would be compromised.

(2) Subject to *subsection (13)*, a member of the Permanent Defence Force not below the rank of commandant may apply to a superior officer for an authorisation under this section where the member believes on reasonable grounds that—

(*a*) *paragraph (a)* or *(b)* of *section 6A(2)* applies to the *Schedule 2* data in respect of which the application is made, and (b) it is likely that, before the Schedule 2 data could be obtained pursuant to an authorisation under *section 6A*—

(i) the data would be wholly or partly destroyed or otherwise rendered unavailable, or

(ii) the security of the State would be likely to be compromised.

(*b*) it is likely that, before the Schedule 2 data could be obtained pursuant to an authorisation under *section 6A*—

(i) the data would be wholly or partly destroyed or otherwise rendered unavailable, or

(ii) the security of the State would be likely to be compromised.

(3) A superior officer to whom an application under *subsection (1)* or *(2)* is made shall issue an authorisation under this section only if satisfied that—

(*a*) *paragraphs (a)* and *(b)* of the subsection concerned apply in respect of the *Schedule 2* data concerned, and

(*b*) the issuing of the authorisation is necessary for, and proportionate to, the purposes for which the application is made.

(4) An authorisation under this section shall authorise the applicant concerned, at any time in the period during which the authorisation has effect, to require the service provider specified in the authorisation to disclose to the applicant *Schedule 2* data—

(*a*) of such class or classes as are specified in the authorisation and in the service provider's possession or control, and

(*b*) subject to such conditions and directions as may be specified in the authorisation.

(5) For the purposes of *subsection (4)(a)*, a superior officer may specify a class or classes of *Schedule 2* data by reference to one or more of the following:

(*a*) a particular location or locations;

(*b*) a particular geographical area or areas;

(*c*) a particular period of time;

(*d*) a particular means of communication;

(*e*) a particular person or particular persons;

(*f*) such other matter or feature as the superior officer considers appropriate.

(6) A superior officer shall, not later than 8 hours after he or she issues an authorisation under this section, prepare a record in writing, in such form as may be prescribed, of the authorisation.

(7) (*a*) A superior officer shall, not later than 7 days after he or she issues an authorisation under this section, prepare a report in relation to the issuing of the authorisation.

(*b*) The record prepared in accordance with *subsection (6)* in relation to an authorisation shall be included in the report prepared under this section in relation to that authorisation.

(8) A report prepared under *subsection (7)* shall:

(*a*) in relation to an authorisation issued pursuant to an application under *subsection (1)*, be submitted by the superior officer concerned to a member of the Garda Síochána not below the rank of chief superintendent;

(*b*) in relation to an authorisation issued pursuant to an application under *subsection (2)*, be submitted by the superior officer concerned to a member of the Permanent Defence Force not below the rank of colonel.

(9) F19**[**Subject to *subsection (15)*, a superior officer**]** shall, as soon as possible and, in any event, not later than 72 hours after he or she issues an authorisation under this section, apply to an authorising judge for affirmation of the authorisation.

(10) An application under *subsection (9)* for affirmation of an authorisation shall—

(*a*) be made F19**[***ex parte*,**]**

(*b*) be upon information on oath, specifying the grounds on which the authorisation was F19**[**issued, and**]**

F20**[**(*c*) be heard otherwise than in public.**]**

(11) An authorising judge, on hearing an application under *subsection (9)*, shall consider whether the authorisation was necessary for, and proportionate to, the purposes for which it was issued and may—

(*a*) affirm,

(*b*) vary, or

(*c*) revoke,

the authorisation.

(12) An authorising judge who revokes, under *subsection (11)(c)*, an authorisation, may, where he or she considers it reasonable to do so, apply to the referee referred to in *section 10* to conduct an investigation under that section in relation to the matter.

(13) An application for an authorisation under this section shall not be made to a superior officer who has had any involvement in the investigation, detection or prevention of a threat or apprehended threat to the security of the State that occasioned the making of the application and, accordingly, such a superior officer shall not consider such an application or issue an authorisation upon such an application.

(14) Subject to *subsection (15)*, an authorisation under this section shall cease to have effect upon the expiration of 72 hours from the issue of the authorisation, or such shorter period as the superior officer may specify in the authorisation.

(15) Where, due to exceptional circumstances that are beyond his or her control, a superior officer is unable to make an application under *subsection (9)* within the period specified in that subsection, he or she—

(*a*) may extend the period during which the authorisation concerned shall have effect by such further period as he or she considers necessary for, and

proportionate to, the purposes for which the authorisation was issued, provided that the total period during which an authorisation to which this subsection applies shall have effect shall not exceed 96 hours from the issue of the authorisation, and

(*b*) where he or she extends under *paragraph (a)* the period during which the authorisation shall have effect, shall make an application under F19**[***subsection (9)***]** before the authorisation ceases to have effect.

(16) This section shall apply to *Schedule 2* data irrespective of whether an order under *section 3A* is in effect in relation to such data.**]**

F21**[**Authorisation to require disclosure of internet source data

6C.— (1) A member of the Garda Síochána not below the rank of inspector may apply to an authorising judge for an authorisation under this section where the member is of the belief that the internet source data in respect of which the application is made—

(*a*) relate to a person whom the member suspects, on reasonable grounds of—

(i) having committed a serious offence, or

(ii) presenting an actual or potential threat to the security of the State,

or

(*b*) are otherwise required to be preserved for the purpose of—

(i) preventing, detecting, investigating or prosecuting a serious offence,

(ii) safeguarding the security of the State,

(iii) protecting the life or personal safety of a person, in circumstances where the member believes that there is a serious risk to the life or personal safety of the person, or

(iv) determining the whereabouts of a missing person.

(2) A member of the Permanent Defence Force not below the rank of commandant may apply to an authorising judge for an authorisation under this section where the member is of the belief that the internet source data in respect of which the application is made—

(*a*) relate to a person whom the member suspects, upon reasonable grounds, of presenting an actual or potential threat to the security of the State, or

(*b*) are otherwise required for the purpose of safeguarding the security of the State.

(3) An officer of the Revenue Commissioners not below the rank of assistant principal officer may apply to an authorising judge for an authorisation under this section where the officer is of the belief that the internet source data in respect of which the application is made—

(*a*) relate to a person whom the officer suspects, on reasonable grounds, of having committed a revenue offence, or

(*b*) are otherwise required to be preserved for the purpose of preventing, detecting, investigating or prosecuting a revenue offence.

F22**[**(4) An officer of the Competition and Consumer Protection Commission not below the rank of assistant principal officer may apply to an authorising judge for an authorisation under this section where the officer is of the belief that the internet source data in respect of which the application is made—

(*a*) relate to a person whom the officer suspects, on reasonable grounds, of having committed a competition offence, or

(*b*) are otherwise required to be preserved for the purpose of preventing, detecting, investigating or prosecuting a competition offence.**]**

(5) An application for an authorisation under this section shall—

(*a*) be made *ex parte*,

(*b*) be upon information on oath, specifying the grounds on which the authorisation is sought,

(*c*) specify, by reference to the criteria specified in subsection (8), the terms of the authorisation sought, and

(*d*) be heard otherwise than in public.

(6) An authorising judge, as respects an application for an authorisation under this section, may issue an authorisation only if satisfied that—

(*a*) *paragraph (a)* or *(b)* of *subsections (1), (2), (3)* or *(4)*, as the case may be, applies in respect of the application, and

(*b*) the issuing of the authorisation is necessary for, and proportionate to, the purposes for which the application was made.

(7) An authorisation under this section shall authorise the applicant concerned, at any time in the period during which the authorisation has effect, to require the service provider specified in the authorisation to disclose to that applicant internet source data in the service provider's possession or control—

(*a*) of such class or classes as are specified in the authorisation, and

(*b*) subject to such conditions and directions as may be specified in the authorisation.

(8) For the purposes of *subsection (7)(a)*, an authorising judge may specify a class of internet source data by reference to any one or more of the following:

(*a*) a particular location or locations;

(*b*) a particular geographical area or areas;

(*c*) a particular period or particular periods of time;

(*d*) a particular means of communication;

(*e*) a particular person or particular persons;

(*f*) such other matter as the authorising judge considers appropriate.**]**

F23**[**Authorisation to require disclosure of internet source data in case of urgency

6D.— (1) Subject to *subsection (15)*, a member of the Garda Síochána not below the rank of inspector may apply to a superior officer for an authorisation under this section where the member believes on reasonable grounds that—

(*a*) *paragraph (a)* or *(b)* of *section 6C(1)* apply to the internet source data in respect of which the application is made, and

(*b*) it is likely that, before the internet source data could be obtained pursuant to an authorisation under *section 6C*—

(i) the data would be wholly or partly destroyed or otherwise rendered unavailable,

(ii) the achievement of an objective specified in *section 6C(1)(b)* would be impeded, or

(iii) the security of the State would be compromised.

(2) Subject to *subsection (15)*, a member of the Permanent Defence Force not below the rank of commandant may apply to a superior officer for an authorisation under this section where the member believes on reasonable grounds that—

(*a*) *paragraph (a)* or *(b)* of *section 6C(2)* apply to the internet source data in respect of which the application is made, and

(*b*) it is likely that, before the internet source data could be obtained pursuant to an authorisation under *section 6C*—

(i) the data would be wholly or partly destroyed or otherwise rendered unavailable, or

(ii) the security of the State would be compromised.

(3) Subject to *subsection (15)*, an officer of the Revenue Commissioners not below the rank of assistant principal officer may apply to a superior officer for an authorisation under this section where the officer believes on reasonable grounds that—

(*a*) *paragraph (a)* or *(b)* of *section 6C(3)* applies to the internet source data in respect of which the application is made, and

(*b*) it is likely that, before the internet source data could be obtained pursuant to an authorisation under *section 6C*—

(i) the data would be wholly or partly destroyed or otherwise rendered unavailable, or

(ii) the prevention, detection, investigation or prosecution of a revenue offence would be impeded.

F24**[**(4) Subject to *subsection (15)*, an officer of the Competition and Consumer Protection Commission not below the rank of assistant principal officer may apply to a superior officer for an authorisation under this section where the officer believes on reasonable grounds that—

(*a*) *paragraph (a)* or *(b)* of *section 6C(4)* apply to the internet source data in respect of which the application is made, and

(*b*) it is likely that, before the internet source data could be obtained pursuant to an authorisation under *section 6C*—

(i) the data would be wholly or partly destroyed or otherwise rendered unavailable, or

(ii) the prevention, detection, investigation or prosecution of a competition offence would be impeded.**]**

(5) A superior officer to whom an application under *subsection (1)*, *(2)*, *(3)* or *(4)* is made shall issue an authorisation under this section only if satisfied that—

(*a*) *paragraphs (a)* and *(b)* of the subsection concerned apply in respect of the internet source data concerned, and

(*b*) the issuing of the authorisation is necessary for, and proportionate to, the purposes for which the application is made.

(6) An authorisation under this section shall authorise the applicant concerned, at any time in the period during which the authorisation has effect, to require the service

provider specified in the authorisation to disclose to the applicant internet source data—

(*a*) of such class or classes as are specified in the authorisation and in the service provider's possession or control, and

(*b*) subject to such conditions and directions as may be specified in the authorisation.

(7) For the purposes of *subsection (6)(a)*, a superior officer may specify a class or classes of internet source data by reference to one or more of the following:

(*a*) a particular location or locations;

(*b*) a particular geographical area or areas;

(*c*) a particular period of time;

(*d*) a particular means of communication;

(*e*) a particular person or particular persons;

(*f*) such other matter or feature as the superior officer considers appropriate.

(8) A superior officer shall, not later than 8 hours after he or she issues an authorisation under this section, prepare a record in writing, in such form as may be prescribed, of the authorisation.

(9) (*a*) A superior officer shall, not later than 7 days after he or she issues an authorisation under this section, prepare a report in relation to the issuing of the authorisation.

(*b*) The record prepared in accordance with *subsection (8)* in relation to an authorisation shall be included in the report prepared under this section in relation to that authorisation.

(10) A report prepared under *subsection (9)* shall:

(*a*) in relation to an authorisation issued pursuant to an application under *subsection (1*), be submitted by the superior officer concerned to a member of the Garda Síochána not below the rank of chief superintendent;

(*b*) in relation to an authorisation issued pursuant to an application under *subsection (2)*, be submitted by the superior officer concerned to a member of the Permanent Defence Force not below the rank of colonel;

(*c*) in relation to an authorisation issued pursuant to an application under *subsection (3)*, be submitted by the superior officer concerned to an officer of the Revenue Commissioners not below the rank of assistant secretary general;

F24**[**(*d*) in relation to an authorisation issued pursuant to an application under *subsection (4)*, be submitted by the superior officer concerned to an officer of the Competition and Consumer Protection Commission not below the rank of member of the Commission.**]**

(11) F25**[**Subject to *subsection (17)*, a superior officer**]** shall, as soon as possible and, in any event, not later than 72 hours after he or she issues an authorisation under this section, apply to an authorising judge for affirmation of the authorisation.

(12) An application under *subsection (11)* for affirmation of an authorisation shall—

(*a*) be made F25**[***ex parte*,**]**

(*b*) be upon information on oath, specifying the grounds on which the authorisation was F25**[**issued, and**]**

F26**[**(*c*) be heard otherwise than in public.**]**

(13) An authorising judge, on hearing an application under *subsection (11)*, shall consider whether the authorisation was necessary for, and proportionate to, the purposes for which it was issued and may—

(*a*) affirm,

(*b*) vary, or

(*c*) revoke,

the authorisation.

(14) An authorising judge who revokes, under *subsection (13)(c)*, an authorisation, may, where he or she considers it reasonable to do so, apply to the referee referred to in *section 10* to conduct an investigation under that section in relation to the matter.

(15) An application for an authorisation under this section shall not be made to a superior officer who has had any involvement in the investigation, detection or prevention of a—

(*a*) threat or apprehended threat to the security of the State, or

(*b*) serious offence, revenue offence or competition offence,

that occasioned the making of the application and, accordingly, such a superior officer shall not consider such an application or issue an authorisation upon such an application.

(16) Subject to *subsection (17)*, an authorisation under this section shall cease to have effect upon the expiration of 72 hours from the issue of the authorisation, or such shorter period as the superior officer may specify in the authorisation.

(17) Where, due to exceptional circumstances that are beyond his or her control, a superior officer is unable to make an application under *subsection (11)* within the period specified in that subsection, he or she—

(*a*) may extend the period during which the authorisation concerned shall have effect by such further period as he or she considers necessary for, and proportionate to, the purposes for which the authorisation was issued, provided that the total period during which an authorisation to which this subsection applies shall have effect shall not exceed 96 hours from the issue of the authorisation, and

(*b*) where he or she extends under *paragraph (a)* the period during which the authorisation shall have effect, shall make an application under *subsection (11)* before the authorisation ceases to have effect.**]**

F27**[**Requirement to disclose cell site location data in case of urgency

6E.— (1) A member of the Garda Síochána not below the rank of inspector may apply to a superior officer for an authorisation under this section where the member believes on reasonable grounds that the cell site location data in respect of which the application was made are required for the purpose of—

(*a*) protecting the life or personal safety of a person, in circumstances where the member believes that there is a serious risk to the life or personal safety of the person, or

(*b*) determining the whereabouts of a missing person.

(2) A superior officer to whom an application under *subsection (1)* is made shall issue an authorisation under this section only if satisfied that—

(*a*) *paragraphs (a)* or *(b)* of the subsection applies in respect of the cell site location data concerned, and

(*b*) the issuing of the authorisation is necessary for, and proportionate to, the purposes for which the application is made.

(3) *Subsections (6)* to *(12)* and *subsections (14)* to *(16)* of *section 6B* shall apply in respect of an authorisation under this section as they apply in respect of an authorisation under that section.

(4) An authorisation under this section shall authorise the applicant concerned, at any time in the period during which the authorisation has effect, to require the service provider specified in the authorisation to disclose to that applicant cell site location data—

(*a*) specified in the authorisation, and

(*b*) subject to such conditions and directions as may be specified in the authorisation.

(5) In this F28**[**section and *section 6F*,**]** "cell site location data" mean data processed by means of an electronic communications network that identifies the most recent geographic location of the device or equipment used by a user when availing of a publicly available electronic communications service.**]**

F29**[**Requirement to disclose *Schedule 2* data, internet source data or cell site location data

6F.— (1) A member of the Garda Síochána, member of the Permanent Defence Force, officer of the Revenue Commissioners or officer of the Competition and Consumer Protection F30**[**Commission**]**, as the case may be, to whom an authorisation has been issued under *section 6A, 6B, 6C, 6D* or *6E* may at any time in the period during which the authorisation has effect, by notice in writing require the service provider specified in the authorisation to F30**[**disclose to the member or officer concerned *Schedule 2* data, internet source data or cell site location data, as the case may be**]**—

(*a*) of such class or classes as are specified in the authorisation and in the service provider's possession or control, and

(*b*) subject to such conditions and directions as may be specified in the authorisation.

(2) A service provider to whom a notice is given under *subsection (1)* shall comply with the requirement concerned—

(*a*) where the disclosure requirement is made pursuant to an authorisation under *section 6B, 6D* or *6E*, without delay, and

(*b*) in any other case, as soon as is practicable.

(3) A member or officer referred to in *subsection (1)* shall, when he or she gives the notice under that subsection to the service provider concerned, give to the service provider a true copy of the authorisation pursuant to which the disclosure requirement is made.

(4) In proceedings for an offence, a document that purports to be a true copy of an authorisation under *section 6A, 6B, 6C, 6D* or *6E* shall be admissible in evidence without further proof.

(5) For the purposes of this section, a document shall be deemed to be a true copy of an authorisation under *section 6A, 6B, 6C, 6D* or *6E* if it has been certified as being a true copy of that authorisation by an authorising judge.**]**

Service provider to comply with disclosure request.

7.—F31**[**...**]**

F32**[**Preservation order in respect of certain *Schedule 2* data

7A.— (1) Without prejudice to *section 3A*, a member of the Garda Síochána not below the rank of inspector may apply to an authorising judge for a preservation order under *subsection (3)* where the member is of the belief that the *Schedule 2* data in respect of which the application is made—

(*a*) relate to a person whom the member suspects, on reasonable grounds of presenting an actual or potential threat to the security of the State, or

(*b*) are otherwise required to be preserved for the purpose of safeguarding the security of the State.

(2) Without prejudice to *section 3A*, a member of the Permanent Defence Forces not below the rank of commandant may apply to an authorising judge for a preservation order under *subsection (3)* where the member is of the belief that the *Schedule 2* data in respect of which the application is made—

(*a*) relate to a person whom the member suspects, on reasonable grounds, of presenting an actual or potential threat to the security of the State, or

(*b*) are otherwise required to be preserved for the purpose of safeguarding the security of the State.

(3) An authorising judge, as respects an application under *subsection (1)* or *(2)*, may make a preservation order under this subsection only if satisfied that—

(*a*) *paragraph (a)* or *(b)* of *subsection (1)* or *(2)*, as the case may be, applies to the *Schedule 2* data in respect of which the application is made, and

(*b*) the issuing of the order is necessary for, and proportionate to, the purposes for which the application is made.

(4) A preservation order under *subsection (3)* may be made in respect of *Schedule 2* data within the following categories:

(*a*) such data stored by a service provider on the basis of Articles 5, 6 and 9 of Directive 2002/58[3];

(*b*) such data stored, retained or otherwise within the possession or control of a service provider under a contractual obligation or pursuant to a court order, including an order under *section 3A* or a preservation order under this Act, and

(*c*) such data, not referred to in *paragraphs (a)* or *(b)*, being data the preservation of which the applicant is legally entitled to request, as may be specified by the authorising judge in the preservation order.

(5) Without prejudice to *section 3A*, a member of the Garda Síochána not below the rank of inspector may apply to an authorising judge for a preservation order under *subsection (8)* where the member is of the belief that the *Schedule 2* data in respect of which the application is made—

(*a*) relate to a person whom the member suspects, on reasonable grounds of having committed a serious offence, or

(*b*) are otherwise required to be preserved for the purpose of—

(i) preventing, detecting, investigating or prosecuting a serious offence,

[3] O.J. No. L201, 31.07.2003, p.37

(ii) protecting the life or personal safety of a person, in circumstances where the member believes that there is a serious risk to the life or personal safety of the person, or

(iii) determining the whereabouts of a missing person.

(6) Without prejudice to *section 3A*, an officer of the Revenue Commissioners not below the rank of assistant principal officer may apply to an authorising judge for a preservation order under *subsection (8)* where the officer is of the belief that the *Schedule 2* data in respect of which the application is made—

(*a*) relate to a person whom the officer suspects, on reasonable grounds, of having committed a revenue offence, or

(*b*) are otherwise required to be preserved for the purpose of preventing, detecting, investigating or prosecuting a revenue offence.

F33**[**(7) Without prejudice to *section 3A*, an officer of the Competition and Consumer Protection Commission not below the rank of assistant principal officer may apply to an authorising judge for a preservation order under *subsection (8)* where the F34**[**officer**]** is of the belief that the *Schedule 2* data in respect of which the application is made—

(*a*) relate to a person whom the officer suspects, on reasonable grounds, of having committed a competition offence, or

(*b*) are otherwise required to be preserved for the purpose of preventing, detecting, investigating or prosecuting a competition offence.**]**

(8) An authorising judge, as respects an application under *subsection (5), (6)* or *(7)*, may make a preservation order under this subsection only if satisfied that—

(*a*) *paragraph (a)* or *(b)* of *subsection (5), (6)* or *(7)*, as the case may be, applies to the *Schedule 2* data in respect of which the application is made, and

(*b*) the issuing of the order is necessary for, and proportionate to, the purposes for which the application is made.

(9) A preservation order under *subsection (8)* may be made in respect of *Schedule 2* data within the following categories:

(*a*) such data stored by a service provider on the basis of Articles 5, 6 and 9 of Directive 2002/58[4],

(*b*) such data stored, retained or otherwise within the possession or control of a service provider under a contractual obligation or pursuant to a court order, other than a order under *section 3A* or a preservation order under *subsection (4)*, and

(*c*) such data, not referred to in *paragraphs (a)* or *(b)*, being data that the applicant is legally entitled to request the preservation of which, as may be specified by the authorising judge in the preservation order.

(10) An application under this section shall—

(*a*) be made ex parte,

(*b*) be upon information on oath, specifying the grounds on which the order is sought,

(*c*) specify, by reference to the criteria specified in *subsection (12)*, the terms of the order sought, and

(*d*) be heard otherwise than in public.

[4] O.J. No. L201, 31.07.2003, p.37

(11) A preservation order under this section, shall, while it is in effect, require the service provider specified in the order to preserve the Schedule 2 data in his or her possession or control—

(*a*) of such category or categories as are, in accordance with *subsection (4)* or *(9)*, specified in the order,

(*b*) such class or classes as are specified in the order, and

(*c*) subject to such conditions and directions as may be specified in the order.

(12) For the purposes of *subsection (11)(a)*, an authorising judge may specify a class or classes of *Schedule 2* data by reference to one or more of the following:

(*a*) a particular location or locations;

(*b*) a particular geographical area or areas;

(*c*) a particular period of time;

(*d*) a particular means of communication;

(*e*) a particular person or particular persons;

(*f*) such other matter or feature as the authorising judge considers appropriate.

(13) A preservation order shall have effect for 90 days, or such lesser period as may be specified in the order.

(14) Where a preservation order is made under this section, the applicant concerned shall, without delay, cause the order to be served on the service provider specified in the order.

(15) A service provider on whom a preservation order under this section is served shall comply with the order.**]**

F35**[**Temporary Preservation Order in respect of certain *Schedule 2* data in case of urgency

7B.— (1) Subject to this section, a member of the Garda Síochána not below the rank of inspector may apply to a superior officer for a temporary preservation order under *subsection (3)* where the member believes on reasonable grounds that—

(*a*) *paragraph (a)* or *(b)* of *section 7A(1)* applies to the *Schedule 2* data in respect of which the application is made, and

(*b*) it is likely that, before the *Schedule 2* data could be obtained pursuant to a preservation order under *section 7A*—

(i) the data would be wholly or partly destroyed or otherwise rendered unavailable, or

(ii) the security of the State would be compromised.

(2) Subject to this section, a member of the Permanent Defence Force not below the rank of commandant may apply to a superior officer for a temporary preservation order under *subsection (3)* where the member believes on reasonable grounds that—

(a) *paragraph (a)* or *(b)* of *section 7A(2)* applies to the Schedule 2 data in respect of which the application is made, and

(*b*) it is likely that, before the *Schedule 2* data could be obtained pursuant to a preservation order under *section 7A*—

(i) the data would be wholly or partly destroyed or otherwise rendered unavailable, or

(ii) the security of the State would be likely to be compromised.

(3) A superior officer to whom an application under *subsection (1)* or *(2)* is made shall make a temporary preservation order under this subsection only if satisfied that—

(*a*) *paragraph (a)* or *(b)* of *subsection (1)* or *(2)*, as the case may be, applies to the *Schedule 2* data in respect of which the application is made, and

(b) the issuing of the order is necessary for, and proportionate to, the purposes for which an application is made.

(4) A temporary preservation order under *subsection (3)* may be made in respect of *Schedule 2* data within the following categories:

(*a*) such data stored by a service provider on the basis of Articles 5, 6 and 9 of Directive 2002/58[5],

(*b*) such data stored, retained or otherwise within the possession or control of a service provider under a contractual obligation or pursuant to a court order, including an order under *section 3A* or a preservation order under this Act, and

(*c*) such data, not referred to in *paragraphs (a)* or *(b)*, being data the preservation of which the applicant is legally entitled to request, as may be specified by the superior officer in the temporary preservation order.

(5) Subject to this section, a member of the Garda Síochána not below the rank of inspector may apply to a superior officer for a temporary preservation order under *subsection (8)* where the member believes on reasonable grounds that—

(*a*) *paragraph (a)* or *(b)* of *section 7A(5)* applies to the *Schedule 2* data in respect of which the application is made, and

(*b*) it is likely that, before the *Schedule 2* data could be obtained pursuant to a preservation order under *section 7A*—

(i) the data would be wholly or partly destroyed or otherwise rendered F36**[**unavailable, or**]**

(ii) the achievement of an objective specified in *section 7A(5)(b)* would be F36**[**impeded.**]**

(iii) F37**[**...**]**

(6) Subject to this section, an officer of the Revenue Commissioners not below the rank of assistant principal officer may apply to a superior officer for a temporary preservation order under *subsection (8)* where the officer believes on reasonable grounds that—

(*a*) *paragraph (a)* or *(b)* of *section 7A(6)* applies to the *Schedule 2* data in respect of which the application is made, and

(*b*) it is likely that, before the *Schedule 2* data could be obtained pursuant to a preservation order under *section 7A*—

(i) the data would be wholly or partly destroyed or otherwise rendered unavailable, or

(ii) the prevention, detection, investigation or prosecution of a revenue offence would be impeded.

F38**[**(7) Subject to this section, an officer of the Competition and Consumer Protection Commission not below the rank of assistant principal officer may apply to a superior officer for a temporary preservation order under *subsection (8)* where the officer believes on reasonable grounds that—

[5] O.J. No. L201, 31.07.2003, p.37

(*a*) *paragraph (a)* or *(b)* of *section 7A(7)* applies to the *Schedule 2* data in respect of which the application is made, and

(*b*) it is likely that, before the *Schedule 2* data could be obtained pursuant to a preservation order under *section 7A*—

(i) the data would be wholly or partly destroyed or otherwise rendered unavailable, or

(ii) the prevention, detection, investigation or prosecution of a competition offence would be impeded.**]**

(8) A superior officer to whom an application under *subsection (5), (6)* or *(7)* is made shall make a temporary preservation order under this subsection only if satisfied that—

(*a*) *paragraph (a)* and *(b)* of *subsection (5), (6)* or *(7)*, as the case may be, apply to the *Schedule 2* data in respect of which the application is made, and

(*b*) the issuing of the order is necessary for, and proportionate to, the purposes for which the application is made.

(9) A temporary preservation order under *subsection (8)* may be made in respect of *Schedule 2* data within the following categories:

(*a*) such data stored by a service provider on the basis of Articles 5, 6 and 9 of Directive 2002/58[6],

(*b*) such data stored, retained or otherwise within the possession or control of a service provider under a contractual obligation or pursuant to a court order, other than an order under *section 3A* or a preservation order under *section 7A(4)*, and

(*c*) such data, not referred to in *paragraphs (a)* or *(b)*, being data the preservation of which the applicant is legally entitled to request to have so specified, as may be specified by the superior officer in the temporary preservation order.

(10) A temporary preservation order under this section shall, while it is in effect, require the service provider specified in the order to preserve the relevant data in his or her possession or control—

(*a*) of such category or categories as are, in accordance with *subsection (4)* or *(9)*, specified in the order,

(*b*) of such class or classes as are specified in the order, and

(*c*) subject to such conditions and directions as may be specified in the order.

(11) For the purposes of *subsection (10)(a)*, a superior officer may specify a class or classes of relevant data by reference to one or more of the following:

(*a*) a particular location or locations;

(*b*) a particular geographical area or areas;

(*c*) a particular period of time, not being more than 90 days, whether starting from the date on which the order is made or such future date as is specified in the order;

(*d*) a particular means of communication;

(*e*) a particular person or particular persons;

(*f*) such other matter or feature as the superior officer considers appropriate.

[6] O.J. No. L201, 31.07.2003, p.37

(12) A superior officer shall, not later than 8 hours after he or she makes an order under this section, prepare a record in writing of the order in such form as may be prescribed.

(13) (*a*) A superior officer shall, not later than 7 days after he or she makes an order under this section, prepare a report in relation to the making of the order.

(*b*) The record prepared in accordance with *subsection (12)* in relation to an order shall be included in the report prepared under this section in relation to that order.

(14) A report prepared under *subsection (13)* shall:

(*a*) in relation to an order made pursuant to an application under *subsection (1)* or *(5)*, be submitted by the superior officer concerned to a member of the Garda Síochána not below the rank of chief superintendent;

(*b*) in relation to an order made pursuant to an application under *subsection (2)*, be submitted by the superior officer concerned to a member of the Permanent Defence Force not below the rank of colonel;

(*c*) in relation to an order made pursuant to an application under *subsection (6)*, be submitted by the superior officer concerned to an officer of the Revenue Commissioners not below the rank of assistant secretary general;

F38**[**(*d*) in relation to an order made pursuant to an application under *subsection (7)*, be submitted by the superior officer concerned to an officer of the Competition and Consumer Protection Commission not below the rank of member of the Commission.**]**

(15) Subject to F36**[***subsection (21)***]**, a superior officer shall, as soon as practicable and, in any event, not later than 72 hours after he or she makes an order under this section, apply to an authorising judge for affirmation of the order.

(16) An application under F36**[***subsection (15)***]** for affirmation of an order shall—

(*a*) be made F36**[***ex parte*,**]**

(*b*) be upon information on oath, specifying the reasons for which the order was F36**[**made, and**]**

F39**[**(*c*) be heard otherwise than in public.**]**

(17) An authorising judge, on hearing an application under *subsection (15)*, shall consider whether the order was necessary for, and proportionate to, the purposes for which it was issued and may—

(*a*) affirm,

(*b*) vary, or

(*c*) revoke,

the order.

(18) An authorising judge who revokes, under *subsection (17)(c)*, an order may, where he or she considers it reasonable to do so, apply to the referee referred to in *section 10* to conduct an investigation under that section in relation to the matter.

(19) An application for an order under this section shall not be made to a superior officer who has had any involvement in the investigation, detection or prevention of a threat or apprehended threat to the security of the State that occasioned the making of the application and, accordingly, such a superior officer shall not consider such an application or make an order upon such an application.

(20) Subject to *subsection (21)*, an order under this section shall cease to have effect upon the expiration of 72 hours from the making of the order, or such shorter period as the superior officer may specify in the order.

(21) Where, due to exceptional circumstances that are beyond his or her control, a superior officer is unable to make an application under *subsection (15)* within the period specified in that subsection, he or she—

(*a*) may extend the period during which the order concerned shall have effect by such further period as he or she considers necessary for, and proportionate to, the purpose for which the order was made, provided that the total period during which an order to which this subsection applies shall have effect shall not exceed 96 hours from the making of the order, and

(*b*) where he or she extends under *paragraph (a)* the period during which the order shall have effect, shall make an application under *subsection (15)* before the order ceases to have effect.

(22) Where a temporary preservation order is made under this section, the applicant concerned shall, without delay, cause the order to be served on the service provider specified in the order.

(23) A service provider on whom a temporary preservation order is served shall comply with the order.**]**

F40**[**Production order in respect of certain *Schedule 2* data

7C.— (1) Without prejudice to *section 3A*, a member of the Garda Síochána not below the rank of inspector may apply to an authorising judge for a production order under *subsection (3)* where the member is of the belief that the *Schedule 2* data in respect of which the application is made—

(*a*) relate to a person whom the member suspects, on reasonable grounds of presenting an actual or potential threat to the security of the State, or

(*b*) are otherwise required to be preserved for the purpose of safeguarding the security of the State.

(2) Without prejudice to *section 3A*, a member of the Permanent Defence Forces not below the rank of commandant may apply to an authorising judge for a production order under *subsection (3)* where the member is of the belief that the *Schedule 2* data in respect of which the application is made—

(*a*) relate to a person whom the member suspects, on reasonable grounds, of presenting an actual or potential threat to the security of the State, or

(*b*) are otherwise required to be preserved for the purpose of safeguarding the security of the State.

(3) An authorising judge, as respects an application under *subsection (1)* or *(2)*, may make a production order under this subsection only if satisfied that—

(*a*) *paragraph (a)* or *(b)* of *subsection (1)* or *(2)*, as the case may be, applies to the *Schedule 2* data in respect of which the application is made, and

(*b*) the issuing of the order is necessary for, and proportionate to, the purposes for which the application is made.

(4) A production order under *subsection (3)* may be made in respect of *Schedule 2* data within the following categories:

(*a*) such data stored by a service provider on the basis of Articles 5, 6 and 9 of Directive 2002/58[7];

[7] O.J. No. L201, 31.07.2003, p.37

(*b*) such data stored, retained or otherwise within the possession or control of a service provider under a contractual obligation or pursuant to a court order, including an order under *section 3A* or a preservation order under this Act, and

(*c*) such data, not referred to in *paragraphs (a)* or *(b)*, being data that the applicant is legally entitled to request, as may be specified by the authorising judge in the production order.

(5) Without prejudice to *section 3A*, a member of the Garda Síochána not below the rank of inspector may apply to an authorising judge for a production order under *subsection (8)* where the member is of the belief that the *Schedule 2* data in respect of which the application is made—

(*a*) relate to a person whom the member suspects, on reasonable grounds of having committed a serious offence, or

(*b*) are otherwise required to be preserved for the purpose of—

(i) preventing, detecting, investigating or prosecuting a serious offence,

(ii) protecting the life or personal safety of a person, in circumstances where the member believes that there is a serious risk to the life or personal safety of the person, or

(iii) determining the whereabouts of a missing person.

(6) Without prejudice to *section 3A*, an officer of the Revenue Commissioners not below the rank of assistant principal officer may apply to an authorising judge for a production order under *subsection (8)* where the officer is of the belief that the *Schedule 2* data in respect of which the application is made—

(*a*) relate to a person whom the officer suspects, on reasonable grounds, of having committed a revenue offence, or

(*b*) are otherwise required to be preserved for the purpose of preventing, detecting, investigating or prosecuting a revenue offence.

F41**[**(7) Without prejudice to *section 3A*, an officer of the Competition and Consumer Protection Commission not below the rank of assistant principal officer may apply to an authorising judge for a production order under *subsection (8)* where the officer is of the belief that the *Schedule 2* data in respect of which the application is made—

(*a*) relate to a person whom the officer suspects, on reasonable grounds, of having committed a competition offence, or

(*b*) are otherwise required to be preserved for the purpose of preventing, detecting, investigating or prosecuting a competition offence.**]**

(8) An authorising judge, as respects an application under *subsection (5), (6)* or *(7)*, may make a production order under this subsection only if satisfied that—

(*a*) *paragraph (a)* or *(b)* of *subsection (5)*, *(6)* or *(7)*, as the case may be, applies to the *Schedule 2* data in respect of which the application is made, and

(*b*) the issuing of the order is necessary for, and proportionate to, the purposes for which the application is made.

(9) A production order under *subsection (8)* may be made in respect of *Schedule 2* data within the following categories:

(*a*) such data stored by a service provider on the basis of Articles 5, 6 and 9 of Directive 2002/58[8];

[8] O.J. No. L201, 31.07.2003, p.37

(*b*) such data stored, retained or otherwise within the possession or control of a service provider under a contractual obligation or pursuant to a court order, other than a order under *section 3A* or a preservation order under *section 7A(4)*, and

(*c*) such data, not referred to in *paragraphs (a)* or *(b)*, being data that the applicant is legally entitled to request, as may be specified by the authorising judge in the production order.

(10) An application under this section shall—

(*a*) be made *ex parte*,

(*b*) be upon information on oath, specifying the grounds on which the order is sought,

(*c*) specify, by reference to the criteria specified in *subsection (12)*, the terms of the order sought, and

(*d*) be heard otherwise than in public.

(11) A production order under this section shall, while it is in effect, require the service provider specified in the order to produce, as soon as is practicable, to the person specified in the order the *Schedule 2* data that in his or her possession or control on the date on which the order is served upon him or her—

(*a*) of such category or categories as are, in accordance with *subsection (4)* or *(9)*, specified in the order,

(*b*) such class or classes as are specified in the order, and

(*c*) subject to such conditions and directions as may be specified in the order.

(12) For the purposes of *subsection (11)(a)*, an authorising judge may specify a class or classes of *Schedule 2* data by reference to one or more of the following:

(*a*) a particular location or locations;

(*b*) a particular geographical area or areas;

(*c*) a particular period of time;

(*d*) a particular means of communication;

(*e*) a particular person or particular persons;

(*f*) such other matter or feature as the authorising judge considers appropriate.

(13) Where a production order is made under this section, the applicant concerned shall, without delay, cause the order to be served on the service provider specified in the order.

(14) A service provider on whom a production order is served shall comply with the order.**]**

F42**[**Temporary Production Order in respect of certain *Schedule 2* data in case of urgency

7D.— (1) Subject to this section, a member of the Garda Síochána not below the rank of inspector may apply to a superior officer for a temporary production order under *subsection (3)* where the member believes on reasonable grounds that—

(*a*) *paragraph (a)* or *(b)* of *section 7C(1)* applies to the *Schedule 2* data in respect of which the application is made, and

(*b*) it is likely that, before the *Schedule 2* data could be obtained pursuant to a production order under *section 7C*—

(i) the data would be wholly or partly destroyed or otherwise rendered unavailable, or

(ii) the security of the State would be compromised.

(2) Subject to this section, a member of the Permanent Defence Force not below the rank of commandant may apply to a superior officer for a temporary production order under *subsection (3)* where the member believes on reasonable grounds that—

(*a*) *paragraph (a)* or *(b)* of *section 7C(2)* applies to the *Schedule 2* data in respect of which the application is made, and

(*b*) it is likely that, before the *Schedule 2* data could be obtained pursuant to a production order under *section 7C*—

(i) the data would be wholly or partly destroyed or otherwise rendered unavailable, or

(ii) the security of the State would be likely to be compromised.

(3) A superior officer to whom an application under *subsection (1)* or *(2)* is made shall make a temporary production order under this subsection only if satisfied that—

(*a*) *paragraph (a)* or *(b)* of *subsection (1)* or *(2)*, as the case may be, applies to the *Schedule 2* data in respect of which the application is made, and

(*b*) the issuing of the order is necessary for, and proportionate to, the purposes for which the application is made.

(4) A temporary production order under *subsection (3)* may be made in respect of *Schedule 2* data within the following categories:

(*a*) such data stored by a service provider on the basis of Articles 5, 6 and 9 of Directive 2002/58[9];

(*b*) such data stored, retained or otherwise within the possession or control of a service provider under a contractual obligation or pursuant to a court order, including an order under section 3A or a preservation order under this Act, and

(*c*) such data, not referred to in *paragraphs (a)* or *(b)*, being data that the applicant is legally entitled to request, as may be specified by the superior officer in the temporary production order.

(5) Subject to this section, a member of the Garda Síochána not below the rank of inspector may apply to a superior officer for a temporary production order under *subsection (8)* where the member believes on reasonable grounds that—

(*a*) *paragraph (a)* or *(b)* of *section 7C(5)* applies to the *Schedule 2* data in respect of which the application is made, and

(*b*) it is likely that, before the *Schedule 2* data could be obtained pursuant to a preservation order under *section 7C*—

(i) the data would be wholly or partly destroyed or otherwise rendered F43**[**unavailable, or**]**

(ii) the achievement of an objective specified in *section 7C(5)(b)* would be F43**[**impeded.**]**

(iii) F44**[**...**]**

(6) Subject to this section, an officer of the Revenue Commissioners not below the rank of assistant principal officer may apply to a superior officer for a temporary

[9] O.J. No. L201, 31.07.2003, p.37

production order under *subsection (8)* where the officer believes on reasonable grounds that—

(*a*) *paragraph (a)* or *(b)* of *section 7C(6)* applies to the *Schedule 2* data in respect of which the application is made, and

(*b*) it is likely that, before the *Schedule 2* data could be obtained pursuant to a production order under *section 7C*—

(i) the data would be wholly or partly destroyed or otherwise rendered unavailable, or

(ii) the prevention, detection, investigation or prosecution of a revenue offence would be impeded.

F45**[**(7) Subject to this section, an officer of the Competition and Consumer Protection Commission not below the rank of assistant principal officer may apply to a superior officer for a temporary production order under *subsection (8)* where the officer believes on reasonable grounds that—

(*a*) *paragraph (a)* or *(b)* of *section 7C(7)* applies to the *Schedule 2* data in respect of which the application is made, and

(*b*) it is likely that, before the *Schedule 2* data could be obtained pursuant to a production order under *section 7C*—

(i) the data would be wholly or partly destroyed or otherwise rendered unavailable, or

(ii) the prevention, detection, investigation or prosecution of a competition offence would be impeded.**]**

(8) A superior officer to whom an application under *subsection (5), (6)* or *(7)* is made shall make a temporary production order under this subsection only if satisfied that—

(*a*) *paragraph (a)* or *(b)* of *subsection (5), (6)* or *(7)*, as the case may be, applies to the *Schedule 2* data in respect of which the application is made, and

(*b*) the issuing of the order is necessary for, and proportionate to, the purposes for which the application is made.

(9) A temporary production order under *subsection (8)* may be made in respect of *Schedule 2* data within the following categories:

(*a*) such data stored by a service provider on the basis of Articles 5, 6 and 9 of Directive 2002/58[10];

(*b*) such data stored, retained or otherwise within the possession or control of a service provider under a contractual obligation or pursuant to a court order, other than an order under *section 3A* or a preservation order under *section 7A(4)*, and

(*c*) such data, not referred to in *paragraphs (a)* or *(b)*, being data that the applicant is legally entitled to request, as may be specified by the superior officer in the temporary production order.

(10) A temporary production order under this section shall, while it is in effect, require the service provider specified in the order to produce to the person specified in the order the *Schedule 2* data in his or her possession or control on the date on which the order is served on him or her—

(*a*) of such category or categories as are, in accordance with *subsection (4)* or *(9)*, specified in the order,

[10] O.J. No. L201, 31.07.2003, p.37

(*b*) of such class or classes as are specified in the order, and

(*c*) subject to such conditions and directions as may be specified in the order.

(11) For the purposes of *subsection (10)(a)*, a superior officer may specify a class or classes of relevant data by reference to one or more of the following:

(*a*) a particular location or locations;

(*b*) a particular geographical area or areas;

(*c*) a particular period of time, not being more than 90 days, whether starting from the date on which the order is made or such future date as is specified in the order;

(*d*) a particular means of communication;

(*e*) a particular person or particular persons;

(*f*) such other matter or feature as the superior officer considers appropriate.

(12) A superior officer shall, not later than 8 hours after he or she makes an order under this section, prepare a record in writing of the order in such form as may be prescribed.

(13) (*a*) A superior officer shall, not later than 7 days after he or she makes an order under this section, prepare a report in relation to the making of the order.

(*b*) The record prepared in accordance with *subsection (12)* in relation to an order shall be included in the report prepared under this section in relation to that order.

(14) A report prepared under *subsection (13)* shall:

(*a*) in relation to an order made pursuant to an application under *subsection (1)* or *(5)*, be submitted by the superior officer concerned to a member of the Garda Síochána not below the rank of chief superintendent;

(*b*) in relation to an order made pursuant to an application under *subsection (2)*, be submitted by the superior officer concerned to a member of the Permanent Defence Force not below the rank of colonel;

(*c*) in relation to an order made pursuant to an application under *subsection (6)*, be submitted by the superior officer concerned to an officer of the Revenue Commissioners not below the rank of assistant secretary general;

F45**[**(*d*) in relation to an order made pursuant to an application under *subsection (7)*, be submitted by the superior officer concerned to an officer of the Competition and Consumer Protection Commission not below the rank of member of the Commission.**]**

(15) Subject to *subsection (21)*, a superior officer shall, as soon as practicable and, in any event, not later than 72 hours after he or she makes an order under this section, apply to an authorising judge for affirmation of the order.

(16) An application under *subsection (15)* for affirmation of an order shall—

(*a*) be made F43**[***ex parte*,**]**

(*b*) be upon information on oath, specifying the reasons for which the order was F43**[**made, and**]**

F46**[**(*c*) be heard otherwise than in public.**]**

(17) An authorising judge, on hearing an application under *subsection (15)*, shall consider whether the order was necessary for, and proportionate to, the purposes for which it was issued and may—

(*a*) affirm,

(*b*) vary, or

(*c*) revoke,

the order.

(18) An authorising judge who revokes, under *subsection (17)(c)*, an order may, where he or she considers it reasonable to do so, apply to the referee referred to in *section 10* to conduct an investigation under that section in relation to the matter.

(19) An application for an order under this section shall not be made to a superior officer who has had any involvement in the investigation, detection or prevention of—

(*a*) threat or apprehended threat to the security of the State, or

(*b*) serious offence, revenue offence or competition offence,

that occasioned the making of the application and, accordingly, such a superior officer shall not consider such an application or make an order upon such an application.

(20) Subject to *subsection (21)*, an order under this section shall cease to have effect upon the expiration of 72 hours from the making of the order, or such shorter period as the superior officer may specify in the order.

(21) Where, due to exceptional circumstances that are beyond his or her control, a superior officer is unable to make an application under *subsection (15)* within the period specified in that subsection, he or she—

(*a*) may extend the period during which the order concerned shall have effect by such further period as he or she considers necessary for, and proportionate to, the purpose for which the order was made, provided that the total period during which an order to which this subsection applies shall have effect shall not exceed 96 hours from the making of the order, and

(*b*) where he or she extends under *paragraph (a)* the period during which the order shall have effect, shall make an application under *subsection (15)* before the order ceases to have effect.

(22) Where a temporary production order is made under this section, the applicant concerned shall, without delay, cause the order to be served on the service provider specified in the order.

(23) A service provider on whom a temporary production order is served shall comply with the order.**]**

Processing for other purpose.

8.— Where all or part of the period specified in a data retention request coincides with the period during which any of the data specified in the request may, in accordance with law, be processed for purposes other than those specified in the request, nothing in *section 6* shall prevent those data from being processed for those other purposes.

Statistics.

9.— (1) The Garda Commissioner shall prepare and submit a report to the Minister in respect of data specified in *Schedule 2* that were the subject of all F47**[**disclosure requirements made by a member of the Garda Síochána under *section 6(1), 6F(1),* F48**[***7C* or *7D***]]** during the relevant period.

(2) The Chief of Staff of the Permanent Defence Force shall prepare and submit a report to the Minister for Defence in respect of data specified in *Schedule 2* that were the subject of all F47**[**disclosure requirements made under *section 6(2), 6F(1),* F48**[***7C* or *7D***]]** during the relevant period.

(3) The Revenue Commissioners shall prepare and submit a report to the Minister for Finance in respect of data specified in *Schedule 2* that were the subject of all F47**[**disclosure requirements made under *section 6(3), 6F(1),* F48**[***7C* or *7D***]]** during the relevant period.

F49**[**(3A) The Competition and Consumer Protection Commission shall prepare and submit a report to the Minister for Jobs, Enterprise and Innovation in respect of data specified in *Schedule 2* that were the subject of all F47**[**disclosure requirements made under *section 6(4), 6F(1),* F48**[***7C* or *7D***]]** during the relevant period.**]**

(4) A report under F50**[***subsection (1), (2), (3)* or *(3A)***]** shall be submitted as soon as is practicable after the end of the relevant period.

(5) The report shall include—

(*a*) the number of times when data had been disclosed in response to a F47**[**disclosure requirement**]**,

(*b*) the number of times when a F47**[**disclosure requirement**]** could not be met,

(*c*) the average period of time between the date on which the retained data were first processed and the F48**[**date on which the disclosure requirement was made**]**.

(6) The Minister for Defence shall review the report submitted under *subsection (2)* and shall forward it to the Minister, along with any comments that he or she may have with respect to it.

(7) The Minister for Finance shall review the report submitted under *subsection (3)* and shall forward it to the Minister, along with any comments that he or she may have with respect to it.

F49**[**(7A) The Minister for Jobs, Enterprise and Innovation shall review the report submitted under *subsection (3A)* and shall forward it to the Minister, along with any comments that he or she may have with respect to it.**]**

(8) The Minister, on receipt of the report submitted under *subsection (1)* and the reports forwarded to him or her under F50**[***subsections (6), (7)* and *(7A)***]** shall review the reports and the comments and shall prepare a State report that consolidates those reports and submit it to the European Commission.

(9) A State report shall be submitted as soon as is practicable after the end of the relevant period.

(10) The State report shall include the matters referred to in *subsection (5)*.

(11) For the purposes of this section, "relevant period" means—

(*a*) the period beginning on the day on which this Act commences and ending on the 31 December next following that day, and

(*b*) each successive 12 month period.

Complaints procedure.

10.— (1) A contravention of F51**[***section 6, 6A, 6B, 6C, 6D, 6E, 6F, 7C* or *7D***]** in relation to a F51**[**disclosure requirement**]** shall not of itself render that disclosure request invalid or constitute a cause of action at the suit of a person affected by the F51**[**disclosure requirement**]**, but any such contravention shall be subject to investigation in accordance with the subsequent provisions of this section and nothing

in this subsection shall affect a cause of action for the infringement of a constitutional right.

(2) A person who believes that data that relate to the person and that are in the possession of a service provider have been accessed following a F51**[**disclosure requirement**]** may apply to the Referee for an investigation into the matter.

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

(*a*) whether a F51**[**disclosure requirement**]** was made as alleged in the application, and

(*b*) if so, whether any provision of F51**[***section 6, 6A, 6B, 6C, 6D, 6E, 6F, 7C* or *7D***]** has been contravened in relation to the F51**[**disclosure requirement**]**.

(4) If, after investigating the matter, the Referee concludes that a provision of F51**[***section 6, 6A, 6B, 6C, 6D, 6E, 6F, 7C* or *7D***]** has been contravened, the Referee shall—

(*a*) notify the applicant in writing of that conclusion, and

(*b*) make a report of the Referee's findings to the Taoiseach.

(5) In addition, in the circumstances specified in *subsection (4)*, the Referee may, if he or she thinks fit, by order do either or both of the following—

F52**[***(a)* direct An Garda Síochána, the Permanent Defence Force, the Revenue Commissioners or the Competition and Consumer Protection Commission to destroy the relevant data and any copies of the data,**]**

(*b*) make a recommendation for the payment to the applicant of such sum by way of compensation as may be specified in the order.

(6) The Minister shall implement any recommendation under *subsection (5) (b)*.

(7) If, after investigating the matter, the Referee concludes that *section 6* has not been contravened, the Referee shall notify the applicant in writing to that effect.

(8) A decision of the Referee under this section is final.

(9) For the purpose of an investigation under this section, the Referee is entitled to access, and has the power to inspect, any official documents or records relating to the relevant application.

(10) Any person who was concerned in, or has information relevant to, the making of a F51**[**disclosure requirement**]** in respect of which an application is made under this section shall give the Referee, on his or her request, such information relating to F53**[**the requirement**]** as is in the person's possession.

Amendment of section 8 (Review of operation of Act by judge of High Court) of Act of 1993.

11.— Section 8 of 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 *section 12* of the *Communications (Retention of Data) Act 2011* 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 2011*.

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

Duties of designated judge in relation to this Act.

12.— (1) 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 Act under review,

F54**[***(b)* ascertain whether An Garda Síochána, the Permanent Defence Force, the Revenue Commissioners 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 Act that the designated judge considers appropriate.

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

(*a*) has the power to investigate any case in which a F55**[**disclosure requirement**]** is made, and

(*b*) may access and inspect any official documents or records relating to the F56**[**requirement**]**.

(3) Any person who was concerned in, or has information relevant to, the preparation or making of a F55**[**disclosure requirement**]** shall give the designated judge, on his or her request, such information relating to F56**[**the requirement**]** as is in the person's possession.

F57**[**(4) The designated judge may, if he or she considers it desirable to do so, communicate with the Taoiseach or the Minister concerning F56**[**disclosure requirements**]** and with the Data Protection Commission in connection with its functions under the Data Protection Regulation and the Data Protection Acts 1988 to 2018.

(5) In this section, "Data Protection Regulation" means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016[39] on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).**]**

F58**[**Offences

12A.— (1) A person who contravenes F59**[***section***]** *3(1), 3A(7), 3B(1), 6(8), 6F(2), 7A(15), 7B(23), 7C(14)* or *7D(23)* shall be guilty of an offence.

(2) A person guilty of an offence under this section shall be liable—

(*a*) on summary conviction, to a class A fine or imprisonment for a term not exceeding 12 months or both, or

(*b*) on conviction on indictment, to a fine not exceeding €500,000 or imprisonment for a term not exceeding 5 years or both.

(3) In proceedings for an offence under *subsection (1)*, it shall be a defence for a person against whom such proceedings are brought to prove that the person took all reasonable steps and exercised all due diligence to avoid the commission of the offence.

(4) Where an offence under this section is committed by a body corporate and is proved to have been committed with the consent or connivance of, or to be attributable to any neglect on the part of, a person being a director, manager, secretary or other officer of the body corporate or a person who was purporting to act in any such capacity, that person, as well as the body corporate, shall be guilty of that offence and shall be liable to be proceeded against and punished as if he or she were guilty of the first-mentioned offence.**]**

[39] OJ No. L 119, 4.5.2016, p.1

F60[Amendment of *Schedule 2*

12B.— (1) The Minister may, following consultation with the Minister for Environment, Climate and Communications and in accordance with this section, by regulation amend *Schedule 2*, where he or she is satisfied that it is necessary to do so in order to ensure that the matters specified in the Schedule adequately reflect developments in electronic communications technology and include data transmitted by means of such technology.

(2) The Minister in exercising the power under *subsection (1)*, may consult with such persons possessing expertise in the area of electronic communications technology as he or she considers appropriate.**]**

F61[Guidelines

12C.— The Minister may issue guidelines—

(*a*) to persons with respect to the making of applications under *sections 7A, 7B, 7C* and *7D*, and

(*b*) to facilitate compliance by service providers with preservation and production orders.**]**

F62[Retention of data

12D.— A service provider who is required under *section 3(1), 3A(5), 3B(1), 7A(11)* or *7B(10)* to retain or, as may be appropriate, preserve data shall retain or preserve, as the case may be, those data—

(*a*) in such a way that they may be disclosed without undue delay pursuant to a disclosure request, and

(*b*) in accordance with regulations, if any, under *section 12F(2)(a)*.**]**

F63[Criteria for specification of geographic area

12E.— A person who, under a provision of this Act, specifies a class or classes of *Schedule 2* data by reference to a particular geographical area or areas, shall do so by reference to criteria that are objective and non-discriminatory and, for that purpose, shall have regard to the criteria specified in regulations under *section 12F(2)(b)* (if any).**]**

F64[Regulations

12F.— (1) The Minister may by regulations provide for any matter referred to in this Act as prescribed or to be prescribed.

(2) The Minister may by regulations provide for one or more of the following:

(*a*) the technical requirements to be met by a person who is obliged under this Act to retain or preserve data, including the requirements to be met so as to ensure that data so retained or preserved, when required under this Act to be disclosed—

(i) may be disclosed without delay, and

(ii) are of sufficient quality to be used for the purposes for which the disclosure is required;

(*b*) the criteria, which shall be objective and non-discriminatory, to which a person shall have regard when specifying a class or classes of *Schedule 2* data by reference to a particular geographic area, which may include:

(i) the rate of crime in an area;

(ii) the number of persons normally present in the area;

(iii) the presence in the area of strategic infrastructure;

F65[(*c*) the procedures for making a requirement under *section 6* or *6F* and for making an application under *section 6A, 6B, 6C, 6D, 6E, 7A, 7B, 7C* or *7D*.**]**

(3) Without prejudice to any provision of this Act, regulations under this section may contain such incidental, supplementary and consequential provisions as appear to the Minister to be necessary or expedient for the purposes of the regulations.

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

F66**[**Notification of data subject

12G. (1) Subject to *subsection (2)*, where *Schedule 2* data have been disclosed to a person pursuant to a requirement under *section 6F(1), 7C* or *7D*, the Garda Commissioner, the Chief of Staff of the Defence Forces, the Chairman of the Revenue Commissioners, the Chairperson of the Competition and Consumer Protection Commission, as may be appropriate, shall, in accordance with regulations under this section, cause to be given to the person to whom the data relate a notice in writing informing him or her of the disclosure of the data concerned.

(2) Without prejudice to the generality of *subsection (1)*, regulations under this section may provide for any one or more of the following:

(*a*) the form of the notice to be given under *subsection (1)*;

(*b*) the information to be provided in that notice, including—

(i) the date on which the *Schedule 2* data were disclosed pursuant to the requirement concerned,

(ii) the date on which the requirement was made, and

(iii) the date of the authorisation under *section 6A* or *6B*, the production order under *section 7C* or temporary production order under *section 7D*, in respect of the data;

(*c*) the persons who shall be consulted before such a notice is given in accordance with this section;

(*d*) the determination of the point in time and circumstances in which a notice should be given having regard to the overriding consideration that this section shall not operate to—

(i) impede the prevention, detection, investigation or prosecution of any serious offence,

(ii) undermine the security of the State, or

(iii) endanger the life or personal safety of any person;

(*e*) the classes of information that shall not be included in a notice under *subsection (1)* having regard to the overriding consideration referred to in *paragraph (d)*;

(*f*) the categories of persons (other than the person to whom the data relate) whose interests are materially affected by the disclosure of traffic and location data pursuant to a disclosure requirement.

(3) This section shall not apply to *Schedule 2* data that have been disclosed in compliance with a disclosure requirement made pursuant to—

(*a*) an authorisation issued under *section 6A(5)*,

F67**[**(*b*) an authorisation issued under *section 6B*,**]**

(*c*) a production order made under *section 7C(3)*, or

F67**[**(*d*) a temporary production order made under *section 7D(3)*.**]]**

F68**[**Service of documents

12H.— (1) A notice or other document that is required to be served on or given to a person under this Act shall be addressed to the person concerned by name and shall be so served on or given to the person—

(*a*) by electronic means,

(*b*) by delivering it to the person,

(*c*) by leaving it at the address at which the person ordinarily resides or carries on business or, in a case in which an address for service has been furnished, at that address,

(*d*) by sending it by post in a prepaid registered letter or by any other form of recorded delivery service to the address referred to in *paragraph (c)*.

(2) For the purposes of this section, a company within the meaning of the Companies Act 2014 is deemed to be ordinarily resident at its registered office, and every other body corporate and every unincorporated body of persons shall be deemed to be ordinarily resident at its principal office or place of business.**]**

F69**[**Processing of personal data

12I. Personal data that are disclosed to a member of the Garda Síochána, a member of the Permanent Defence Forces, an officer of the Revenue Commissioners or an officer of the Competition and Consumer Protection F70**[**Commission**]**, pursuant to a requirement under *section 6(1)*, F71**[**...**]**, *6F(1), 7C(11)* or *7D(10)* made for the purposes of the prevention, detection, investigation or prosecution of criminal offences, shall be processed in accordance with Part 5 of the Data Protection Act 2018.**]**

F72**[**Provisions relating to authorising judge

12J. (1) The President of the District Court shall designate such and so many judges of the District Court to be authorising judges for the purposes of this Act.

(2) An application to an authorising judge under F73**[***section***]** *6A, 6B, 6C, 6D, 7A, 7B, 7C* or *7D* may be made—

(*a*) whether or not the service provider in respect of whom the authorisation is issued is resident or located in the District Court district to which the authorising judge stands assigned, and

(*b*) whether or not the data to which the authorisation applies is retained by the service provider within the District Court district to which the authorising judge stands assigned.**]**

Repeal.

13.— (1) Part 7 of the Criminal Justice (Terrorist Offences) Act 2005 is repealed.

(2) Notwithstanding the repeal under *subsection (1)*, data that were the subject of a data retention request under Part 7 of the Criminal Justice (Terrorist Offences) Act 2005 before that repeal may be adduced in evidence in proceedings conducted after that repeal subject to the provisions of this Act applying and having effect.

F74**[**Transitional provision

13A.— Where, immediately before the date on which *section 10* of the Communications (Retention of Data) (Amendment) Act 2022 comes into operation, data is retained by a service provider pursuant to the service provider's obligation under *section 3* (before its amendment by section 3 of the Communications (Retention of Data) (Amendment) Act 2022), the service provider shall, on and from that date, and for the purposes of compliance with disclosure requirements made pursuant to

an authorisation under *section 6A* or *6B*, continue to retain such data until the earlier of the following events:

(*a*) the expiry of a period of 6 months beginning on that date, or

(*b*) the making of the first order under *section 3A*.**]**

Short title.

14.— This Act may be cited as the Communications (Retention of Data) Act 2011.

Section 1.

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 1995.

5. An offence under section 5 of the Protections for Persons Reporting Child Abuse Act 1998.

F75**[**6. An offence under Regulation 5 or 7 of the European Union (Market Abuse) Regulations 2016.**]**

Section 3.

SCHEDULE 2

PART 1

Fixed network telephony and mobile telephony data to be retained under section 3

1. Data necessary to trace and identify the source of a communication:

(*a*) the calling telephone number;

(*b*) the name and address of the subscriber or registered user.

2. Data necessary to identify the destination of a communication:

(*a*) the number dialled (the telephone number called) and, in cases involving supplementary services such as call forwarding or call transfer, the number or numbers to which the call is routed;

(*b*) the name and address of the subscriber or registered user.

3. Data necessary to identify the date and time of the start and end of a communication.

4. Data necessary to identify the type of communication:

the telephone service used.

5. Data necessary to identify users' communications equipment or what purports to be their equipment:

(*a*) the calling and called telephone number;

(*b*) the International Mobile Subscriber Identifier (IMSI) of the called and calling parties (mobile telephony only);

(*c*) the International Mobile Equipment Identity (IMEI) of the called and calling parties (mobile telephony only);

(*d*) in the case of pre-paid anonymous services, the date and time of the initial activation of the service and the cell ID from which the service was activated (mobile telephony only).

6. Data necessary (mobile telephony only) to identify the location of mobile communication equipment:

(*a*) the cell ID at the start of the communication;

(*b*) data identifying the geographical location of cells by reference to their cell ID during the period for which communication data are retained.

PART 2

Internet access, Internet e-mail and Internet telephony data to be retained under section 3

1. Data necessary to trace and identify the source of a communication:

(*a*) the user ID allocated;

(*b*) the user ID and telephone number allocated to any communication entering the public telephone network;

(*c*) the name and address of the subscriber or registered user to whom an Internet Protocol (IP) address, user ID or telephone number was allocated at the time of the communication.

2. Data necessary to identify the destination of a communication:

(*a*) the user ID or telephone number of the intended recipient of an Internet telephony call;

(*b*) the name and address of the subscriber or registered user and user ID of the intended recipient of the communication.

3. Data necessary to identify the date, time and duration of a communication:

(*a*) the date and time of the log-in and log-off of the Internet access service, based on a certain time zone, together with the IP address, whether dynamic or static, allocated by the Internet access service provider to a communication, and the user ID of the subscriber or registered user;

(*b*) the date and time of the log-in and log-off of the Internet e-mail service or Internet telephony service, based on a certain time zone.

4. Data necessary to identify the type of communication:

the Internet service used.

5. Data necessary to identify users' communication equipment or what purports to be their equipment:

(*a*) the calling telephone number for dial-up access;

(*b*) the digital subscriber line (DSL) or other end point of the originator of the communication.

Number 3 *of* 2011

COMMUNICATIONS (RETENTION OF DATA) ACT 2011

REVISED

Updated to 1 August 2023

About this Revised Act

This Revised Act presents the text of the Act as it has been amended since enactment, and preserves the format in which it was passed.

Related legislation

Communications (Retention of Data) Acts 2011 and 2014: this Act is one of a group of Acts included in this collective citation, to be construed together as one (*Competition and Consumer Protection Act 2014* (29/2014), s. 1(4)). The Acts in this group are:

- *Communications (Retention of Data Act 2011* (3/2011)
- *Competition and Consumer Protection Act 2014* (29/2014), s. 89

Annotations

This Revised Act is not annotated and only shows textual amendments. An annotated version of this revision is also available which shows textual and non-textual amendments and their sources. It also shows editorial notes including statutory instruments made pursuant to the Act and previous affecting provisions.

Material not updated in this revision

Where other legislation is amended by this Act, those amendments may have been superseded by other amendments in other legislation, or the amended legislation may have been repealed or revoked. This information is not represented in this revision but will be reflected in a revision of the amended legislation if one is available.

A list of legislative changes to any Act, and to statutory instruments from 1972, may be found linked from the page of the Act or statutory instrument at www.irishstatutebook.ie.