Number 25 *of* 2022

Communications (Retention of Data) (Amendment) Act 2022

Number 25 *of* 2022

COMMUNICATIONS (RETENTION OF DATA) (AMENDMENT) ACT 2022

CONTENTS

Section

1. Definition
2. Amendment of section 1(1) of Principal Act
3. Amendment of section 3 of Principal Act
4. Insertion of sections 3A and 3B in Principal Act
5. Amendment of section 6 of Principal Act
6. Insertion of sections 6A to 6F in Principal Act
7. Insertion of sections 7A to 7D in Principal Act
8. Insertion of sections 12A to 12J in Principal Act
9. Transitional provision
10. Miscellaneous amendments of Principal Act
11. Short title and commencement

ACTS REFERRED TO

Communications (Retention of Data) Act 2011 (No. 3)

Companies Act 2014 (No. 38)

Data Protection Act 2018 (No. 7)

Number 25 *of* 2022

COMMUNICATIONS (RETENTION OF DATA) (AMENDMENT) ACT 2022

An Act to amend the Communications (Retention of Data) Act 2011; to provide for the retention in specified circumstances by providers of electronic communications services of certain data; to provide for the disclosure in specified circumstances of such data and to provide for related matters. [21*st July,* 2022]

Be it enacted by the Oireachtas as follows:

Definition

1. In this Act, "Principal Act" means the Communications (Retention of Data) Act 2011.

Amendment of section 1(1) of Principal Act

2. Section 1(1) of the Principal Act is amended—

(a) by the substitution of the following definition for the definition of "user":

> " '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;",

and

(b) by the deletion of the definition of "disclosure request"; and

(c) by the insertion of the following definitions:

> " 'authorising judge' means a judge of the District Court designated under section 12J(1);
>
> '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—
>
> (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;

'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;

'Schedule 2 data' means the categories of data specified in Parts 1 and 2 of Schedule 2;

'superior officer' means—

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

(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;

(d) in relation to an officer of the Competition and Consumer Protection Authority, an officer of the Competition and Consumer Protection Authority not below the rank of principal officer;

'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;".

Amendment of section 3 of Principal Act

3. The Principal Act is amended by the substitution of the following section for section 3—

"Obligation to retain user 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.".

Insertion of sections 3A and 3B in Principal Act

4. The Principal Act is amended by the insertion of the following sections after section 3—

"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 Schedule 2 data, are stored in the State, or in the case of data specified in Part 2 of Schedule 2 data, 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.

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).".

Amendment of section 6 of Principal Act

5. The Principal Act is amended by the substitution of the following section for section 6—

"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.

(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 member 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 member 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.".

Insertion of sections 6A to 6F in Principal Act

6. The Principal Act is amended by the insertion of the following section after section 6A:

"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.

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.

(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) 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 *ex parte*, and

(b) be upon information on oath, specifying the grounds on which the authorisation was issued.

(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 subsection (10) 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.

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.

(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.

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.

(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;

(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) 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 *ex parte*, and

(b) be upon information on oath, specifying the grounds on which the authorisation was issued.

(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.

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 section, '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.

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 Authority, 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 disclose to the member Schedule 2 data or, as the case may be, 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.

(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.".

Insertion of sections 7A to 7D in Principal Act

7. The Principal Act is amended by the insertion of the following sections after section 7:

"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,

(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—

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

(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.

(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 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 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,

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

(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 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.

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—

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

(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 unavailable,

(ii) the achievement of an objective specified in section 7A(5)(b) would be impeded, or

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

(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.

(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—

(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;

(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 (18), 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 (21) for affirmation of an order shall—

(a) be made *ex parte*, and

(b) be upon information on oath, specifying the reasons for which the order was made.

(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.

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];

(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—

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

(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.

(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];

(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.

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

(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.

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 unavailable,

(ii) the achievement of an objective specified in section 7C(5)(b) would be impeded, or

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

(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 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.

(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—

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

(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,

(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.

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

(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;

(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 *ex parte*, and

(b) be upon information on oath, specifying the reasons for which the order was made.

(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.".

Insertion of sections 12A to 12J in Principal Act

8. The Principal Act is amended by the insertion of the following sections after section 12:

"Offences

12A. (1) A person who contravenes sections 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.

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.

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.

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).

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).

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;

(c) the procedures for making an application under sections 6, 6A, 6B, 6C, 6D, 6E, 6F, 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.

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),

(b) an authorisation affirmed or varied under section 6B(11),

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

(d) a production order affirmed or varied under section 7D(17).

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.

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 Authority, pursuant to a requirement under section 6(1), 6E(1), 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.

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 sections 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.".

Transitional provision

9. The Principal Act is amended by the insertion of the following section after section 13:

"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.".

Miscellaneous amendments of Principal Act

10. (1) Section 4(1) of the Principal Act is amended:

(a) by the substitution of "section 3(1), 3A(5), 3B(1), 7A(11) or 7B(10)" for "section 3(1)", and

(b) by the substitution of the following paragraph for paragraph (d):

"(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) Section 5(b) of the Principal Act is amended by the substitution of "disclosure requirement" for "disclosure request".

(3) The Principal Act is amended by the deletion of section 7.

(4) Section 9 of the Principal Act is amended—

(a) in subsection (1), by the substitution of "disclosure requirements made by a member of the Garda Síochána under section 6(1), 6F(1), 7C(1) or 7D(1)" for "disclosure requests made under section 6(1)",

(b) in subsection (2), by the substitution of "disclosure requirements made under section 6(2), 6F(1), 7C(2) or 7D(2)" for "disclosure requests made under section 6(2)",

(c) in subsection (3), by the substitution of "disclosure requirements made under section 6(3), 6F(1), 7C(6) or 7D(6)" for "disclosure requests made under section 6(3)",

(d) in subsection (3A), by the substitution of "disclosure requirements made under section 6(4), 6F(1), 7C(7) or 7D(7)" for "disclosure requests made under section 6(3A)", and

(e) in subsection (5) by the substitution of "disclosure requirement" for "disclosure request" in each place in which it occurs.

(5) Section 10 of the Principal Act is amended—

(a) by the substitution of "disclosure requirement" for "disclosure request" in each place in which it occurs,

(b) in subsection (1), by the substitution of "section 6, 6A, 6B, 6C, 6D, 6E, 6F, 7C or 7D" for "section 6",

(c) in subsection (3), by the substitution of "section 6, 6A, 6B, 6C, 6D, 6E, 6F, 7C or 7D" for "section 6", and

(d) in subsection (4), by the substitution of "section 6, 6A, 6B, 6C, 6D, 6E, 6F, 7C or 7D" for "section 6".

(6) Section 12 of the Principal Act is amended by the substitution of "disclosure requirement" for "disclosure request" in each place in which it occurs.

Short title and commencement

11. (1) This Act may be cited as the Communications (Retention of Data) (Amendment) Act 2022.

(2) This Act shall come into operation on such day or days as the Minister for Justice may appoint by order or orders either generally or with reference to any particular purpose

or provision and different days may be so appointed for different purposes or different provisions.