Number 3 of 2011

COMMUNICATIONS (RETENTION OF DATA) ACT 2011
REVISED
Updated to 25 May 2018

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 Data Protection Act 2018 (7/2018), enacted 24 May 2018, and all statutory instruments up to and including Data Protection Act 2018 (Establishment Day) Order 2018 (S.I. No. 175 of 2018), made 24 May 2018, were considered in the preparation of this Revised Act.

Disclaimer: While every care has been taken in the preparation of this Revised Act, the Law Reform Commission can assume no responsibility for and give no guarantees, undertakings or warranties concerning the accuracy, completeness or up to date nature of the information provided and does not accept any liability whatsoever arising from any errors or omissions. Please notify any errors, omissions and comments by email to revisedacts@lawreform.ie.
Introduction

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 annotated and includes textual and non-textual amendments, statutory instruments made pursuant to the Act and previous affecting provisions.

An explanation of how to read annotations is available at www.lawreform.ie/annotations.

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Where other legislation is amended by this Act, those amendments may have been superseded by other amendments in other legislation, or the amended legislation may have been repealed or revoked.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.

Where legislation or a fragment of legislation is referred to in annotations, changes to this legislation or fragment may not be reflected in this revision but will be reflected in a revision of the legislation referred to if one is available.

A list of legislative changes to any Act, and to statutory instruments from 1985, may be found linked from the page of the Act or statutory instrument at www.irishstatutebook.ie.
Acts which affect or previously affected this revision

- Data Protection Act 2018 (7/2018)
- Freedom of Information Act 2014 (30/2014)
- Competition and Consumer Protection Act 2014 (29/2014)

All Acts up to and including Data Protection Act 2018 (7/2018), enacted 24 May 2018, were considered in the preparation of this revision.

Statutory instruments which affect or previously affected this revision

- European Union (Market Abuse) Regulations 2016 (S.I. No. 349 of 2016)
- Finance (Transfer of Departmental Administration and Ministerial Functions) Order 2011 (S.I. No. 418 of 2011)

All statutory instruments up to and including Data Protection Act 2018 (Establishment Day) Order 2018 (S.I. No. 175 of 2018), made 24 May 2018, were considered in the preparation of this revision.
Number 3 of 2011

COMMUNICATIONS (RETENTION OF DATA) ACT 2011

REVISED

Updated to 25 May 2018

ARRANGEMENT OF SECTIONS

Section
1. Interpretation.
3. Obligation to retain data.
4. Data security.
5. Access to data.
6. Disclosure request.
7. Service provider to comply with disclosure request.
8. Processing for other purpose.
12. Duties of designated judge in relation to this Act.
13. Repeal.

SCHEDULE 1
Offences Deemed to be Serious Offences

SCHEDULE 2
PART 1

FIXED NETWORK TELEPHONY AND MOBILE TELEPHONY DATA TO BE RETAINED UNDER SECTION 3

PART 2
INTERNET ACCESS, INTERNET E-MAIL AND INTERNET TELEPHONY DATA TO BE RETAINED UNDER SECTION 3

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
Finance Act 1999 2001, No. 7
Finance Act 2001 2003, No. 3
Finance Act 2003 2005, No. 5
Finance Act 2005
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
Taxes Consolidation Act 1997 1997, No. 39

[26th January, 2011]

BE IT ENACTED BY THE OIREACHTAS AS FOLLOWS:

Annotations

Modifications (not altering text):

C1 Records under Act excluded from application of Freedom of Information Act (30/2014) (14.10.2014) by Freedom of Information Act 2014 (30/2014), s. 42(b)(x), commenced as per s. 1(2).

Restriction of Act

42.—This Act does not apply to— ...

(b) a record held or created by the Garda Síochána that relates to any of the following: ...

(x) the Communications (Retention of Data) Act 2011,

...

Interpretation.

1.— (1) In this Act—

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

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

F1 [‘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;]

1 O.J. No. L105, 13.04.2006, p. 54

“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;

“disclosure request” means a request to a service provider under section 6 for the disclosure of data retained in accordance with section 3;

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

“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;
(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;

“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;

“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;

“user” means a person using a publicly available electronic communications service, for private or business purposes, without necessarily having subscribed to that service;

“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.
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.

3.— (1) A service provider shall retain data in the categories specified in Schedule 2, for a period of 2 years in respect of the data referred to in Part 1 of Schedule 2 and for a period of one year in respect of the data referred to in Part 2 of Schedule 2.

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

(a) in the case of data that before the passing of this Act were the subject of a data retention request under Part 7 of the Criminal Justice (Terrorist Offences) Act 2005, on the date before the passing of this Act on which the data were first processed by the service provider,

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

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

(4) The data referred to in subsection (1) include data relating to unsuccessful call attempts that, in the case of data specified in Part 1 of Schedule 2, are stored in the State, or in the case of data specified in Part 2 of Schedule 2, are logged in the State.

(5) This section does not require a service provider to retain aggregated data, data that have been made anonymous or data relating to unconnected calls.

(6) In this section “aggregated data” means data that cannot be related to individual subscribers or users.

4.— (1) A service provider who retains data under section 3 (1) shall take the following security measures in relation to the retained data:

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

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

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

(d) the data, except those that have been accessed and preserved, shall be destroyed by the service provider after—

(i) in the case of the data in the categories specified in Part 1 of Schedule 2, a period of 2 years and one month, or
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 disclosure request,

(c) in accordance with a court order, or

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

Disclosure request.

6.— (1) A member of the Garda Síochána not below the rank of chief superintendent may request a service provider to disclose to that member data retained by the service provider in accordance with section 3 where that member is satisfied that the data are required for—

(a) the prevention, detection, investigation or prosecution of a serious offence,

(b) the safeguarding of the security of the State,

(c) the saving of human life.

(2) An officer of the Permanent Defence Force not below the rank of colonel may request a service provider to disclose to that officer data retained by the service provider in accordance with section 3 where that officer is satisfied that the data are 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 request a service provider to disclose to that officer data retained by the service provider in accordance with section 3 where that officer is satisfied that the data are required for the prevention, detection, investigation or prosecution of a revenue offence.

F2[(3A) A member of the Competition and Consumer Protection Commission may request a service provider to disclose to that member data retained by the service provider in accordance with section 3 where that member is satisfied that the data are required for the prevention, detection, investigation or prosecution of a competition offence.]

(4) A disclosure request shall be made in writing, but in cases of exceptional urgency the request may be made orally (whether by telephone or otherwise) by a person entitled under F3[subsection (1), (2), (3) or (3A)] to make the request.

(5) A person who makes a disclosure request orally shall confirm the request in writing to the service provider within 2 working days of the request being made.

Annotations

Amendments:

Service provider to comply with disclosure request.

7.— A service provider shall comply with a disclosure request made to the service provider.

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 disclosure requests made under section 6(1) 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 disclosure requests made under section 6(2) 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 disclosure requests made under section 6(3) during the relevant period.

F4[(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 disclosure requests made under section 6(3A) during the relevant period.]

(4) A report under F5[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 disclosure request,

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

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

(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.

F4[(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 F5[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.
A State report shall be submitted as soon as is practicable after the end of the relevant period.

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

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.
10.— (1) A contravention of section 6 in relation to a disclosure request shall not of itself render that disclosure request invalid or constitute a cause of action at the suit of a person affected by the disclosure request, 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 disclosure request 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 disclosure request was made as alleged in the application, and

(b) if so, whether any provision of section 6 has been contravened in relation to the disclosure request.

(4) If, after investigating the matter, the Referee concludes that a provision of section 6 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—

F6[(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 disclosure request in respect of which an application is made under this section shall give the Referee, on his or her request, such information relating to the request as is in the person’s possession.

Annotations

Amendments:

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,

(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 disclosure request is made, and

(b) may access and inspect any official documents or records relating to the request.

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

(4) The designated judge may, if he or she considers it desirable to do so, communicate with the Taoiseach or the Minister concerning disclosure requests 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 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).]
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.

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.
3. An offence under section 12 of the Non-Fatal Offences against the Person Act 1997.

F9[6. An offence under Regulation 5 or 7 of the European Union (Market Abuse) Regulations 2016.]

Annotations

Amendments:

F9 Inserted (3.07.2016) by European Union (Market Abuse) Regulations 2016 (S.I. No. 349 of 2016), reg. 52, in effect as per reg. 1(2).

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.
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.