Memorandum of Understanding (MoU)
between

The Alternative Operators in the Communications Market (ALTO),
Telecommunications and Internet Federation (TIF) and
The Internet Service Providers Association of Ireland (ISPAI)

and the following State agencies:
An Garda Síochána,
The Permanent Defence Forces
The Revenue Commissioners

in relation to
Section 6 of the Communications (Retention of Data) Act 2011

4th May 2011

Memorandum of Understanding (MoU) between the Communications Industry[1] and the following State agencies [2]: An Garda Síochána, The Permanent Defence Forces and The Revenue Commissioners, in relation to Section 6 of the Communications (Retention of Data) Act 2011

Roles of the Communications Industry and State agencies relating to the Communications (Retention of Data) Act 2011, to include provisions of the Data Retention Enforcement Directive 2006/24/EC

Purpose of the MoU

1. The purpose of the MoU is to promote efficient and effective standards of co-operation between the State and the Communications Industry:

    a. in dealing specifically with Section 6 of the Communications (Retention of Data) Act 2011 (hereinafter "the Act");

    b. clarifying of the operating procedures to be utilised by parties to this MoU;

    c. detailing clearly the data to be retained by Undertakings;

    d. protecting the rights of users; and

    e. assisting in the prevention of serious offences, the safeguarding of the security of the State and the saving of human life.

2. This MoU is a non-binding statement of understanding or agreement and creates no legal obligations on the signing parties.

Background

3. This MoU operates on foot of the Act which gives effect to Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006[3] on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC[4], to provide for the retention and access to certain data for the purposes of the prevention of serious offences, the safeguarding of the security of the State and the saving of human life. The Act repeals the Criminal Justice (Terrorist Offences) Act 2005, part 7, and amends the Interception of Postal Packets and Telecommunications Messages (Regulation) Act 1993.

4. This MoU does not operate to counter or contradict the legislative intent of the European Institutions or the Houses of the Oireachtas.

---

[1] Represented by: The Alternative Operators in the Communications Market (ALTO), Telecommunications and Internet Federation (TIF) and The Internet Service Providers Association of Ireland (ISPAI). These groups are all industry associations, without prejudice to, or excluding any unrepresented communications Undertaking in the State. The expression 'Undertaking' shall be used to mean: Authorised operator, service provider or legal Undertaking

[2] At the time of signing

[3] O.J. No. L105, 13.04.2006 p. 54

[4] O.J. No. L201, 31.07.2002 p. 37

5. This MoU takes effect subject but not limited to, other legislative instruments[5] mentioned in the Act. Nothing in the MoU can prejudice the Act as compliance with the Act will always take precedence over the MoU.

6. This MoU sets out an understanding by the parties regarding implementation of the Act and in particular the details of data to be retained by members of the signatory industry associations. This MoU shall be considered to foster best industry practice.

7. This MoU seeks to minimise the costs, time delay and audit requirements of complying with data access requests under the Act and to promote efficient administration of its requirements within the Communications Industry working with agencies of the State.

8. This MoU is intended to make formulation, transmission, verification and servicing of applications for data disclosure requests as efficient as possible and to ensure that an audit trail specifically relating to requests received exists.

Applicability

9. This MoU specifically mentions Undertakings. This MoU is applicable regardless of the requirement or preference to be Authorised[6] under the Electronic Communications Networks and Services. In most cases Undertakings will be subject to Authorisation requirements.

10. This applicability statement in no way fetters the discretion or powers of State agencies in the lawful conduct of criminal investigations.

11. This MoU applies across the mobile network operator, fixed line network operator and Internet Service Provider – ISP, markets[7].

12. Fixed and mobile Undertakings will already be operating in compliance with existing laws in the area of data retention. Modifications brought about as a result of the Act should be read in line with the annexes and schedules to this MoU.

---

[5] Criminal Assets Bureau Act 1996 – 1996, No. 31
Criminal Evidence Act 1992 – 1992, No. 12
Criminal Justice (Terrorist Offences) Act 2005 – 2005, No. 2
Customs Consolidation Act 1876, 39 & 40, Vict. Ch. 36
Data Protection Act 1988 – 1988, No. 25
Data Protection Acts 1988 and 2003
Finance Act 1999 – 1999, No. 2
Finance Act 2001 – 2001, No. 7
Finance Act 2003 – 2003, No. 3
Finance Act 2005 – 2005, No. 5
Interception of Postal Packets and Telecommunications Messages (Regulation) Act 1993 – 1993, No. 10
Non-Fatal Offence Against the Person Act 1997 – 1997, No. 26
Prevention of Corruption Acts 1889 to 1995
Protections for Persons Reporting Child Abuse Act 1998 – 1998, No. 49
Taxes Consolidation Act 1997 – 1997, No. 39

[6] Entities subject to the Act may not be Authorised under the European Communities (Electronic Communications Networks and Services) Authorisation Regulations 2003 S.I. 306 of 2003 transposing Directive 2002/20/EC (as amended), but are also subject to the Act.

[7] In some cases, Irish Undertakings may be providing services in all three markets e.g., Mobile, Fixed and ISP.

13. The Act now includes legal requirements on public ISPs and the ISP divisions of Undertakings, the following points are noted and agreed:

    - An Undertaking shall retain data only in relation to a service that is provided directly by the provider and which is under the provider's operational control;

    - Services provided using the providers network, datacentre, servers or other facilities by a third party, where the provider does not have operational control of the service, shall not be subject to retention by the provider; in this case, retention is the responsibility of the 3rd party;

    - All events will be provided with a timestamp containing a time zone. This will not necessarily be the local time zone; and

    - While retained data may identify IP addresses, endpoint information and or subscriber information presented by a user, providers do not seek to independently verify this information. In addition, providers cannot in general identify the individual actually using a device at a particular time.

14. This MoU contains three detailed schedules which have been agreed by the parties. These schedules are:

    - **Schedule 1:** Data to be retained relating to fixed and mobile network telephony – **Retention period: 2 years**[8];

    - **Schedule 2:** Data to be retained relating to Internet Service Providers (Internet Access, Internet email and Internet Telephony – VoIP) – **Retention period: 1 year**[9]; and

    - **Schedule 3:** Procedures for making and servicing a data request.

Process steps

15. The State agency[10] will contact the relevant Undertaking with lawful application for a data disclosure request under the Act, without undue delay. At this time the agency will undertake to:

    - Provide the Undertaking with the necessary details[11] including a copy of the Written Authorisation[12] or Court Order, necessary to progress the application for data disclosure;

    - Where an oral request is made of an Undertaking the State agency will comply with the obligation under Section 6 Subsection 5[13], of the Act.

---

[8] Refer to Sections 3 and 4 (1)(d)(i) relating to Part 1, Schedule 2 of the Act.
[9] Refer to Sections 3 and 4 (1)(d)(ii) relating to Part 2, Schedule 2 of the Act.
[10] State Agency – meaning the agencies in the title of this MoU and the Act, those being: An Garda Siochana, The Permanent Defence Forces and The Revenue Commissioners. State Agencies may also include those authorised by an Irish Court with an Order.
[11] See Annex Data for details agreed in the case of each Undertaking (Fixed Line, Mobile or ISP).
[12] Whether this be a member of An Garda Siochana not below the rank of Chief Superintendent, a member of the Permanent Defence Forces not below the rank of colonel or a member of the Revenue Commissioners not below the rank of principal officer.

- Request the Undertaking to furnish all of the relevant and necessary detail to progress the application for data disclosure;

- Engage with the nominated contacts, servants or agents of the Undertaking should the Undertaking express concerns as to the complexity of the data disclosure request; and

- Aim to establish and maintain authorised single channels of communication and or contact with the Undertaking.

16. The relevant Undertaking will:

- Provide all relevant data or information requested without undue delay from receipt of the initial contact by an agency of the State, unless the agency requests a desired time for delivery or otherwise agrees a delivery period with the Undertaking;

- Provide any additional information subsequently requested by the State agency without undue delay from the date of receipt of the initial data disclosure request;

- Provide all the information requested, including any information that may have been redacted or separately stored; and

- Record, whether electronically or physically the nature of the lawful application for data disclosure under the Act.

General

17. It is acknowledged by parties to this MoU that systems development, installation and testing requirements differ between Undertakings and that some significant time delays may exist before full compliance is reached within the terms of the Act.

18. Data will only be retained if it is processed by an Undertaking[14].

19. It is agreed that data, except that which has been accessed by agencies of the State shall be destroyed[15] after the statutory retention period,[16] save for retention of data subject to other lawful business purposes.[17]

20. A Technical Working Group[18] will be established to address issues relating to Data Retention and this MoU, in addition to recommending revisions to this MoU as required. The Technical Working Group will meet quarterly or as required.

21. Wherever possible, agencies of the State and the Communications Industry shall communicate by means of electronic communication.

---

[13] *"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".*

[14] If a pre-paid account is unregistered with a service provider, operators will not seek to collect identification data on the user.

[15] Subject to Sections 4 (1d) of the Act.

[16] Please refer to Section 3 (1)

[17] What happens after the retention period to the undertakings' data, which has been disclosed to a State Agency, will be discussed by the technical working group.

[18] To include approved representatives of industry associations and Government Agencies.

22. This MoU shall be kept under review and will be amended, as necessary, in light of experience.

23. The State agencies and the Communications Industry who are party to this MoU shall ensure that this MoU is appropriately disseminated within Government (where necessary) and to the wider Communications Industry.

24. The parties to this MoU shall ensure that all relevant personnel will be fully briefed and trained on this MoU and its implications.

For and on behalf of:

An Garda Síochána

Signature: _____

Print Name: _____

Print Title: _____

The Alternative Operators in the Communications Market – ALTO

Signature: _____

Print Name: _____

Print Title: _____

The Internet Service Providers Association of Ireland – ISPAI

Signature: _____

Print Name: _____

Print Title: _____

The Permanent Defence Forces

Signature: _____

Print Name: _____

Print Title: _____

The Revenue Commissioners

Signature: _____

Print Name: _____

Print Title: _____

The Telecommunications and Internet Federation – TIF

Signature: _____

Print Name: _____

Print Title: _____

Annex 1: Definitions

In this Memorandum of Understanding:

"MoU" means Memorandum of Understanding

"State agency/agencies" means An Garda Síochána, The Permanent Defence Forces, The Revenue Commissioners, The Data Protection Commission

"the Act" means the Communications (Retention of Data) Act 2011, commenced on 26th January 2011.

"Communications Industry" means the industry represented by: ALTO, TIF and ISPAI

"Undertaking" means the collective description for an Authorised operator, service provider or legal undertaking. The Act separately defines the term "service provider"

"parties" means the signatory groups above to include State agency representatives and representative groups from the communications industry

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

"disclosure request" means a request to a service provider under section 6 of the Act for disclosure of data retained in accordance with section 3 of the Act

"service provider" means a person who is engaged in the provision of a publicly available electronic service or a public communications network by means of a fixed line or mobile telephone of the Internet

"written authorisation" or "warrant" means a lawful data disclosure request which is sent from and authorised by a member of An Garda Siochana not below the rank of Chief Superintendent, a member of the Permanent Defence Forces not below the rank of colonel or a member of the Revenue Commissioners not below the rank of principal officer

"Technical Working Group" means a group formed to discuss technical matters arising out of the operation of this MoU

Schedule 1: Data to be retained relating to fixed and mobile network telephony – **Retention period: 2 years**[19]

Text from the Act Schedule 2, Part 1	Mutual agreement of retained data	Issues addressed and agreed
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	The "A" number - MSISDN	
(b) The name and address of the subscriber or registered user	First name. Surname. Service address.	(1) Pre-pay customers need not be registered (2) No verification is done on the validity of data collected by operators (3) No confirmation given as to who was actually using the equipment at the time the communication was made
*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	The "B" number - MSISDN	Where call forwarding is being used an operator would require 2 (or possibly more) requests
(b) The name and address of the subscriber or registered user	First name. Surname. Service address.	(1) Pre-pay customers need not be registered (2) No verification is done on the validity of data collected by operators (3) No confirmation given as to who was actually using the equipment at the time the communication was made
3: Data necessary to identify the date and time of the start and end of a communication.	Date, start time of call and duration of call	(1) "Start time" should be presented to the nearest second (2) "Start time" will be presented in local time format (i.e. local to where the call was made) (3) It is acceptable to provide "start time" and "finish time" instead of "start time" and "duration" - where this option is availed of "finish time" should be to the nearest second. (4) Local time changes (i.e. Spring and Autumn) may cause some issues but it is agreed by all that they are not significant (5) "Time" / "Duration" will cover pick up to hang up (i.e. ringing time will not be recorded)
4. Data necessary to identify the type of communication: the telephone service used.	Type or service is - voice / SMS / MMS / data / video	If MNOs do not differentiate between voice and video on their billing records then the call record type will be shown as voice.
*5. Data necessary to identify users' communication **equipment** or what purports to be their equipment:*		
(a) The calling and called telephone number	The "A" and "B" numbers - MSISDN's	
(b) The International Mobile Subscriber Identifier (IMSI) of the called and calling parties (mobile telephony only)	IMSI	

[19] **Note:** Section 4 (1)(d)(i)

(c) The International Mobile equipment Identity (IMEI) of the called and calling parties (mobile telephony only)	IMEI	
(d) In the case of pre-paid anonymous services, the date and time of the initial activation of the service and the cell ID from which the service was activated (mobile telephony only)	Date and time of initial activation along with associated cell ID	(1) Time should be presented to the nearest second (2) Time will be presented in local time format (i.e. local to where the call was made) (3) Associated cell ID data and date and time of initial activation shall only be retained for 2 years (4) Initial activation is defined as being the first outbound event on the account.
6. Data necessary (mobile telephone only) to identify the ***location*** *of mobile communication equipment:*		
(a) The cell ID at the start of the communication	Originating cell	(1) In areas of National Roaming provision of Location Access Code – LAC, data is acceptable (2) In areas of International Roaming - country of roaming is acceptable (3) Such location data will only be retained for the calling party and not the called party
(b) Data identifying the geographical location of cells by reference to their location cell ID during the period for which communication data are retained.		The data to be provided shall mirror those data being provided by MNOs under the Emergency Call Answering Service – ECAS, regime to date.

Schedule 2: Data to be retained relating to Internet Service Providers (Internet Access, Internet email and Internet Telephony – VoIP) – **Retention period: 1 year**[20].

Text from the Act Schedule 2, Part 2	**Mutual agreement of retained data**		**Issues addressed and agreed**	
	Access	**Email**	**Internet telephony**	
Internet access, Internet e-mail and Internet telephony data to be retained under section 3				Note: Internet Telephony applies to SIP, IAX and other VoIP services excluding DOCSIS; DOCSIS is covered under voice telephony
1. Data necessary to trace and identify the source of a communication:				
(a) the user ID allocated;	Userid if allocated. IMSI or MISDN for MNOs only	Envelope sender email address	SIP: Userid of VoIP subscriber; IAX: trusted	

[20] **Note:** Section 4 (1)(d)(ii)

			IP (if originating from our subscriber)	
(b) the user ID and telephone number allocated to any communication entering the public telephone network;	n/a	n/a	Userid & telephone number (if allocated) for calls placed onto PSTN; also for internet to SMS and Fax gateways	
(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.	Userid and any available personal details of IP address user – where available	Any available personal details of email sender – where sent by our customer	Any available personal details of VoIP user – where this is our customer	NB only available for a user using a service provided by the ISP, not for access, email or VoIP transit-only services
2. Data necessary to identify the destination of a communication:	(as source)			
(a) the user ID or telephone number of the intended recipient of an Internet telephony call;	n/a	n/a	Userid and/or VoIP/IAX next proxy IP address and/or phone number (depending on destination of call)	
(ii) the name and address of the subscriber or registered user and user ID of the intended recipient of the communication.	Userid and any available personal details of IP address user – where available	Any available personal details of email recipient	Any available personal details of VoIP user	NB only available for a user using a service provided by the ISP, not for access, email or VoIP transit-only services
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	Date & time of logon/logoff to access service, IP, MAC or other endpoint information, as further described in (e)(ii). Information not available for some always-on services, specifically leased line and cable access.	n/a	n/a	

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.	n/a	Date. time & IP of email being sent or received by our server; date, time & IP of an email check (but not what messages were retrieved)	Date, time and IP of SIP & IAX registration for our customers –	The granularity of registration data for VoIP is to be agreed. Possible suggestions: most recent registration; daily
4. Data necessary to identify the type of communication:- the Internet service used.	Type of access (dialup/DSL/WLL/Wi-Fi/Cable/leased line, /Mobile Broadband – MBB, etc)	POP3/IMAP/SMTP etc	VoIP to PSTN/VoIP to VoIP, etc within our network; is it SIP or IAX	
5. Data necessary to identify users' communication equipment or what purports to be their equipment:				
(a) the calling telephone number for dial-up access;	Calling telephone number (if presented).	n/a	n/a	
(b) the digital subscriber line (DSL) or other end point of the originator of the communication.	For DSL: phone number and/or DSLAM port (as available). For Wi-Fi or WLL service MAC address; For cable: modem MAC; for mobile: IMEI/IMSI. For other technologies, whatever specific endpoint information is available	n/a	n/a	

Schedule 3: Procedures for making and servicing a data request:

Single point of contact principle

The parties to the MoU and the Undertakings that they represent, undertake to have an authorised single point of contact. All data disclosure requests to and expected from the industry will be made from the State agencies to these units, employees, servants or agents.

The industry associations will maintain a register of contact points of their members.

Electronic communication

As best practice, the parties agree that secure electronic communication of requests and responses will be the preferable method of communication.

The State agencies will provide a unique e-mail address from which requests will be sent. This will be digitally signed and encrypted.

The Undertakings will provide a unique e-mail address at which requests can be received. Responses will also be sent from this address and will be digitally signed and encrypted.

Where for technical or operational reasons communication in this way is not possible, an alternative fax number or emergency telephone number will be provided

Standard request and response formats

The parties will endeavour to develop a standard electronic mail and paper form; however there will be no obligation on signing parties to use that form.