The Voice of Next Generation Communications

Data Retention Guidance

Compliance Guidance supported by ITSPA Associate member:

Introduction

Data retention requirements for communications providers have seen several changes over recent years, due to both legislative developments and legal challenges. This has created some degree of confusion amongst communication providers regarding the requirements they must comply with. This short guide is designed to provide clarity to members in this area.

A brief legal history

The first Act of Parliament on the matter was the Regulation of Investigatory Powers Act 2000 ("**RIPA**"). The "blanket" surveillance in RIPA was underpinned, in part, by Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 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 (and its predecessor legislation) (the "**Retention Directive**").

The Retention Directive was challenged in the Court of Justice of the European Union and found to be incompatible with, *inter alia,* European Human Rights legislation in the Judgment of the Court (Grand Chamber) of 8 April 2014 (requests for a preliminary ruling from the High Court of Ireland (Ireland) and the Verfassungsgerichtshof (Austria)) – Digital Rights Ireland Ltd (C-293/12) v Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, The Commissioner of the Garda Síochána, Ireland and the Attorney General, and Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl and Others (C-594/12) (the "**CJEU Judgment**"). No replacement Directive has yet been proposed.

This led Parliament to pass the Data Retention and Investigatory Powers Act 2014 ("**DRIPA**") which had a sunset clause in it. The idea of DRIPA was that it expressed the will of Parliament such to make the retention of data lawful and compatible with the CJEU Judgment.

DRIPA itself was subject to a legal challenge, brought by two Members of Parliament, which was won in the High Court in *The Queen on Application of David Davis MP and Tom Watson MP and Ors v The Secretary of State for the Home Department* [2015] EWHC 2092 (Admin) (the "**High Court Judgment**")

What legislation must ITSPA members adhere to?

The main piece of legislation that ITSPA members should be aware of is the Investigatory Powers Act 2016 ("**IPA**"). The Act received royal assent on 29 November 2016 and is gradually becoming law. This IPA is the current good law of the day regarding data retention, which replaced DRIPA and will gradually replace RIPA at dates yet to be determined (i.e. different sections of RIPA will continue in force until expressly repealed). In this short guide we will focus on the requirements under IPA, albeit some of them may not be in force just yet.

The IPA covers the interception of communications, the retention and acquisition of communications data, and equipment interference.

With limited exceptions, the investigatory powers provided for in the IPA already existed. The IPA consolidates and updates powers available to the State to obtain relevant communications which were previously provided for in a number of different statutes.

This Act extends to England and Wales, Scotland and Northern Ireland.

The Act itself is subject to legal uncertainty as the Court of Justice of the European Union ("**CJEU**") has handed down a preliminary ruling in a referral from an appeal brought to the Court of Appeal by the Home Secretary to the High Court Judgment. Although the **CJEU** decision concerned DRIPA, it could affect certain aspects of the IPA, such as the collection of internet records.

ITSPA's view on the IPA

ITSPA does not take a view on the balance of privacy versus security; this is for our elected representatives to debate and decide. ITSPA's interest in the IPA (and its predecessors) has been on the technical aspects of the legislation. Our response to the House of Commons Public Bill Committee can be found here.

What does the IPA mean for ITSPA Members?

When it fully comes into force, the IPA will regulate the interception of communications, the retention and acquisition of communications data and equipment interference, which ITSPA members will need to follow and comply with.

Data Retention requirements under the IPA

As regards data retention, the IPA provides powers for the Secretary of State to require, by notice, communication providers to retain "relevant" communications data and provides a new power for the Secretary of State to require, by notice, the retention of internet connection records ("**Retention Notice**").

Communications data is data held by a telecommunications operator or available directly from the network which identifies a person or device on the network, ensures that a communication reaches its intended destination, describes how a person has been using a service or relates to the architecture of the telecommunication system itself. Communications data is divided into entities data (data about persons, groups or objects and links between them) and events data (identifies and describes activities of entities – e.g. persons).

The IPA defines "relevant communications data" as "communications data" which may be used to identify, or assist in identifying, any of the following:

a) the sender or recipient of a communication (whether or not a person);
b) the time or duration of a communication;
c) the type, method or pattern, or fact, of communication;
d) the telecommunication system (or any part of it) from, to or through which, or by means of which, a communication is or may be transmitted; or
e) the location of any such system;

Such communications data include phone numbers, email addresses and source IP addresses, and as stated, this now includes internet connection records.

Internet connection records are the records of the internet services that show when a specific device connects to sources such as a website or instant messaging application, which are captured by the ISP.

However, the relevant Communications data does **not** include the "content" of the communication.

A Retention Notice **must not** require any relevant communications data to be retained for more than **12 months.**

Unless you receive a Retention Notice, you are not required to retain any data under IPA, although you can retain data for your own business purposes in accordance with applicable laws (companies may be required to keep data by other laws but for other purposes, for example GC11 (Metering and Billing) imposes an obligation on CPs to keep certain records). Furthermore, if you don't have it, then you are not required to provide it (this means that a Retention Notice must not require a communications operator who controls or provides a telecommunication system to retain data which is not needed by the system operator for the functioning of the system in relation to that communication or retained by the operator for other lawful purposes). If you've had a Retention Notice served to you under the IPA (or under RIPA, as applicable) you will know about it. It will dictate what you are required to keep, for how long, and also involve a discussion around a contribution to your reasonable costs for the retention of that data.

Finally, remember that "weblogs" is a much-misused expression in the press with regards to the IPA; it really means IP address and port number; whereas a weblog is a far more intrusive set of data and there is much jurisprudence on where in a web address it becomes content and ceases to be "communications data".

A communications operator retaining communications data under a Retention Notice must keep such data secure, protected against unauthorised access and, once the retention period expires, destroy it (unless retained for other lawful purposes).

How will data access requests work under the IPA?

It's quite simple.

If you retain data for business as usual purposes (for example, CDRs for metering and billing under General Condition of Entitlement 11, or consolidated records for VAT purposes), then if you are asked for that data under the IPA, you are required to provide it, but the relevant authority making the request will need to be fully compliant with the IPA and any other applicable legislation.

An authorisation for obtaining data under the IPA ("**Authorisation**") can be granted where a designated senior officer in a relevant public authority (e.g. the police) is content that a request is necessary for one of the 10 purposes specified in IPA and proportionate to what is sought to be achieved. Data cannot be acquired for any other purposes and only certain authorities can use the power for certain purposes.

Conduct to acquire data may involve serving a notice on a communications provider that requires them to: (i) disclose the relevant data; or (ii) obtain and then disclose the relevant data; or (iii) the relevant public authority acquiring the data directly from an operator (through a secure auditable system or directly from a telecommunications system).

An Authorisation cannot authorise the interception of the content of a communication or require the interference with any equipment on a telecommunications network as this would require a warrant.

An Authorisation may cover data that is not in existence at the time of the Authorisation. This allows a relevant public authority to request data on a forward looking basis in respect of a known subject of interest.

Every Authorisation must specify: (i) the position held by the designated senior officer granting the Authorisation; (ii) which of the limited purposes it is being granted for, the conduct for which it was authorised; (iii) the type of data to be obtained, and who the data will be disclosed to; (iv) the name of the operator and the requirements that

will be imposed on that operator; (v) the position held by the person giving the notice; (vi) the requirements that will be imposed on that operator; and (vii) the name of the operator.

An Authorisation ceases to have effect at the end of the period of one month beginning from the date it was granted, but it can be renewed at any period during the month, by following the same procedure as for obtaining a fresh Authorisation. The renewed Authorisation will last for a period of one month from the date the existing Authorisation expires.

Local authorities' Authorisations to obtain communications data can only take effect if approved by a relevant judicial authority.

Data protection aspects

Unless it is anonymised, communications data may allow those who have access to it to identify the subjects of such data. Therefore, communications data will most likely constitute personal data on many occasions.

As a data controller of the personal data contained in the communications data they handle, communication providers have to comply with the Data Protection Act 1998 and must therefore not disclose the personal data of their end users, unless this is adequately requested by a relevant public authority under applicable law (or the end user consents). Communication providers will also need to comply with the confidentially obligations they have towards their customers.

In light of the above, communication providers must assess carefully any data access request they receive for accessing their data and request legal advice where necessary.

DISCLAIMER: This is a brief guidance for information purposes only and is general and educational in nature. The guidance does not intend to constitute legal advice for any specific situation or a definitive or complete statement of the law on any subject. The guidance may not reflect or include all recent legal developments and may not apply to all the specific facts and circumstances of individual transactions and cases. Preiskel & Co LLP and ITSPA do not undertake any obligation to consider whether the information provided in this guidance is sufficient or appropriate for any particular circumstances. You should seek separate legal advice where necessary.

Preiskel & Co LLP
4 King's Bench Walk
Temple
London, EC4Y 7DL
United Kingdom
Tel: +44 (0)207 332 5640
dpreiskel@preiskel.com
jsaras@preiskel.com
www.preiskel.com

ITSPA
69 Wilson Street
London
EC2A 2BB
Tel: +44 (0)20 3397 3312
team@itspa.org.uk
www.itspa.org.uk

About Preiskel & Co

Preiskel & Co is a telecoms and tech boutique law firm based in the City that specialises in UK and international corporate, commercial, litigation, and regulatory matters. The firm is independently recognised as a leader in the telecommunications, media and technology sectors, also possessing significant expertise in intellectual property (including filing patents and trademarks), data privacy, retention and encryption.

Preiskel offers a range of services for a client base that spans from telecoms resellers, MVNOs/MVNAs, through to MNOs, major handset manufacturers and regulators across the telecoms and technology ecosystem. The firm's 4 partners are independently recognised as leaders in the telecoms field and are at the forefront of the sector with much telecoms industry experience between them. For example, Tim Cowen was general counsel for BT's international businesses and is a member of the Competition Appeal Tribunal; Ronnie Preiskel had legal and business

development roles at BT and Vodafone and at a mobile content company, whilst Danny Preiskel was a specialist telecoms investment banker.

About ITSPA

Founded in 2004, ITSPA is a membership-led organisation that represents predominantly network operators, service providers, resellers and other businesses involved with the supply of next generation communications to business and residential consumers within the UK. ITSPA helps act as the voice for the sector to key stakeholders; ensures that standards created by or imposed on industry are fair; leads on developments of best practice; campaigns on key issues that members face, promotes competition and self-regulation and serves as the leading networking forum for the UK VoIP and next generation communications industry with events throughout the year.

Members also receive complimentary subscription to the dispute resolution scheme CISAS; summaries of Ofcom (and other) consultation papers; regulatory briefing documents; Government monitoring and intelligence reports; updates from legal professionals; anti-fraud information; and the opportunity to collaborate with peers to promote career development.