*Below are excerpts (in black) from the current CD Codes of Practice where ‘lawful authority’ is mentioned. Sections 1 and 2 will require amendment to include the new definition of ‘lawful authority’. The proposed changes to text are in red.*

**Section 1 Introduction**

**1.3** Section 12 of the Act (with Schedule 2) abolishes or amends other information gathering powers in law which provided for access to communications data without appropriate safeguards. Accordingly, relevant public authorities for the purposes of Part 3 should not use other statutory powers to obtain communications data from a postal or telecommunications operator unless that power:

· is authorised by a warrant or order issued by a person holding judicial office; or

· deals with telecommunications operators, postal operators, or a class of such operators and can be used either:

o in connection with the regulation of telecommunications operators, telecommunications services or telecommunication systems, or postal operators or services; or

o to acquire communications data relating to postal items crossing the United Kingdom border.

**1.4** Such powers should only be used to obtain communications data from a telecommunications operator or postal operator where it is not possible for the public authority to obtain the communications data under the Act.

**1.5** In addition, relevant public authorities should also not require, or invite, any postal or telecommunications operator to disclose communications data by relying on any exemption to restrictions on disclosing personal data under relevant data protection legislation.

**Section 2 Scope and definitions: Telecommunications operator and postal operator**

**2.11** Where a relevant public authority wishes to acquire data that is both communications data and other information they will need to ensure they have lawful authority for both types of acquisition. Refer to chapter ‘X’ in compliance and offences for the definition of lawful authority.

**2.42** A communications data authorisation cannot authorise a public authority to use a password obtained through that or another communications data authorisation. If a public authority wishes to use a password obtained through a communications data authorisation to access the content of stored communications or any communications service it must, in accordance with section 6

**2.43** of the Act, ensure that it has appropriate lawful authority.

**Section 15 Compliance and offences**

**Offences**

**15.6** The Act creates two offences which are relevant to the acquisition and disclosure of communications data.

**Acquisition Offence**

**New para 15.7**

The purpose of section 11 in the Act is to discourage public authorities from acquiring communications data from telecommunications operators without a clear lawful authority.

Under section 11 of the Act, it is an offence for a person in a public authority listed in Schedule 4 to the Act to knowingly or recklessly to obtain communications data from a telecommunications operator or postal operator without lawful authority.

It did not intend to discourage public authorities from sharing communications data with another public authority where it is necessary and proportionate for them to do so. The section 11 acquisition offence therefore does not apply to public authorities which acquire communications data from another public authority *which is acting as a telecommunications operator in relation to that communications data*.

Public authorities should only seek to acquire targeted communications data from a telecommunications operator without a Part 3 authorisation where:

* it is not reasonably practicable to obtain a Part 3 authorisation;
* the authority is acquiring it for supervisory and regulatory purposes (see paragraphs XX and YY about section 12 IPA);
* the authority has obtained some other independent or judicial authorisation; or
* the CD has already been published by making it available to the public or a section of the public.

Where a public authority has actively sought to obtain targeted communications data lawfully without exercising a statutory power (e.g., by agreement), it should consider informing IPCO at the next inspection.

The following are examples of where a relevant person in a public authority has the appropriate lawful authority to obtain communications data from a telecommunications operator or postal operator. This is a non-exhaustive list of authorities that will amount to “lawful authority”, and which includes the following;

* where the relevant person has obtained the communications data under section 81(1) IPA 2016;
* where the communications data is obtained in the exercise of a statutory power of the relevant public authority, e.g., in the context of a civil investigation or for regulatory or supervisory purposes (refer to section 12 schedule 2 abolition or restriction of general information gathering powers);
* where the telecommunications or postal operator lawfully provides the communications data to the relevant public authority voluntarily,
* any judicial authorisation e.g., a court order or;
* where the data has been obtained after it has been published and made available to the public and;
* where the communications data has been obtained by the relevant person when responding to a call made to the emergency services e.g., when a person has made a call to the police, fire, rescue and ambulance services and His Majesty’s coast guard. This information is normally only available from the telecommunications operator for the period of 60 minutes following that call. After that a Part 3 authorisation will normally be required in relation to that communications data.

**15.8** The creation of the offence of unlawfully obtaining communications data reflects the sensitivity of communications data and the need for careful consideration in authorisation of its acquisition. The roles and responsibilities laid down for the senior responsible officer, designated senior officer and SPoC are designed to prevent the knowing or reckless acquisition of communications by a public authority where it does not hold a lawful authorisation. Proper adherence to the requirements Communications Data Code of Practice 91 of the Act and this code, including following the procedures identified in chapter 4, will mitigate the risk of any offence being committed.

**15.9** The offence is not committed if the person who obtained the communications data can show that they acted in the reasonable belief that they had lawful authority to obtain the data.

**15.10** This offence is not designed to capture errors on behalf of the public authority but rather, for example, instances where a person in a public authority failed to take account of obvious risk or where a person in a public authority deliberately fails to obtain an authorisation or obtains communications data from a telecommunications operator or postal operator despite the fact that they could not have genuinely believed that an authorisation would be in place.

**15.11** In particular, it is not an offence to obtain communications data where it is made publicly or commercially available by the telecommunications operator or postal operator or otherwise where the telecommunications operator or postal operator freely consents to its disclosure. In such circumstances the consent of the operator provides the lawful authority for the obtaining of the data. However, as set out in paragraphs 1.3 – 1.5, relevant public authorities should not require, or invite, any postal or telecommunications operator to disclose communications data by relying on any exemption to restrictions on disclosing personal data under relevant data protection legislation.