GENERAL GUIDANCE NOTE

Guidance on Retention of Data

Who should read this?

All Network operators and providers involved in the provision of premium rate services (PRS) to consumers.

What is the purpose of the Guidance?

To assist network operators and providers in identifying the types of information that are likely to be necessary to retain in order to resolve consumer enquiries and complaints and enable effective progression of PSA enquiries and investigations. To also clarify PSA's expectations on retention periods for various categories of information.

What are the key points?

The main issues covered in this guidance are:

- PSA's expectations on the retention of Relevant Data and Relevant DDRAC Data
- Non-exhaustive examples of specific types of Relevant Data and Relevant DDRAC Data, including personal data, in the following key areas:
    - Data which relates to proof of promotion and/or consent
    - Data which relates to the handling of consumer complaints and enquiries to a provider
    - Data which relates to the due diligence, risk assessment and control which the provider has carried out on parties with whom they contract

Definitions of Relevant Data and Relevant DDRAC Data

1. For the purposes of this Guidance "Relevant Data" is defined as all information held by network operators and providers that relate to the promotion, operation, content and provision of any premium rate service and any other information that may be of evidential value to a PSA enquiry or investigation. "Relevant DDRAC Data" is defined as all records of and information relating to due diligence and risk assessment and control which a Network operator or Level 1 provider has carried out on parties with whom they contract, as well as any related or other information that may be relevant to their provision of phone-paid services and/or of evidential value to a DDRAC investigation.

2. Both Relevant Data and Relevant DDRAC Data may include personal data and may be requested by PSA as part of an enquiry or investigation into the promotion, operation, content or provision of a service, or when considering the due diligence and risk assessment undertaken by a Network operator or Level 1 provider in relation to their clients and/or

services operated by them. The disclosure and retention of such data is governed by law.

3. However, network operators and providers should note that this Guidance sets out expectations around retention of information more broadly, noting that such information may be held by different parties involved in the provision of a phone-paid service. This Guidance covers broader information than personal data because there are other types of information that may have great importance and/or may be of strong evidential value to the PSA during an enquiry or investigation, helping to ensure that it is able to fully understand all the issues and adopt the right approach in addressing any identified harm or market issues.

4. This Guidance applies to all Relevant data and Relevant DDRAC data that was already being held by network operators and providers, prior to this Guidance coming into force.

Disclosure and retention of personal data

5. In considering this Guidance PSA has had full regard to the EU General Data Protection Regulation 2016 (GDPR), and the UK Data Protection Act 2018 (DPA) in respect of personal data. In March 2018 the PSA issued a Notice setting out its position in relation to disclosure of information to PSA under the GDPR and DPA[3]. In summary this was (and remains) that:

- The new data protection laws do not affect a phone-payment provider's ability to provide PSA with personal data when requested under the Code. Article 6(1)(c) of the GDPR states that processing (including storage) will be lawful if:

  > *Processing is necessary for compliance with a legal obligation to which the controller is subject.*

- In terms of further requirements of the first and other principles under the GDPR, paragraph 5(2) of Schedule 2 of the DPA provides an exemption for data controllers in relation to disclosure of personal data where this is done as a result of an enactment. The relevant enactment for providers of phone-paid services is the Communications Act 2003 under which the Code is approved and enforced.

- Where special categories of personal data (referred to as 'sensitive personal data' under the DPA 1998) were concerned, the requirements had not changed: Consumers must give consent to such data being passed to the PSA (with providers expected to make all reasonable efforts to do so).

6. The Notice also stated that in relation to non-special category personal data requested by the PSA at the enquiry stage, the most appropriate legal basis for providers to process such data is the "legitimate interests" basis[4], focussing on the legitimate interests of the provider and/or their consumers. Providers duly relying on the "legitimate interests" basis would not need to seek the consent of individual consumers before providing their data to the PSA.

7. The retention of personal data is governed primarily by the 'data limitation' and 'storage limitation' principles set out within Article 5 of the GDPR. Network operators and providers are required to comply with these principles when retaining personal data. When considering

these principles in relation to the retention of Relevant Data and Relevant DDRAC Data, network operators and providers should take PSA's assessment of the *necessity* requirement of the principles into account.

8. We consider that there is a clear need for providers to ensure that they retain, for a sufficient period, all information that may be necessary to fully assist consumers in the resolution of their enquiries and complaints, including provision of appropriate protection and redress to those consumers suffering detriment from phone-paid services**.** This includes the need for such information to be available for a sufficient period to enable an effective PSA investigation process that works in the interests of both providers and their consumers, ensuring that all relevant evidence is able to be considered.

9. We are clear that the consideration of all relevant evidence undoubtedly leads to fairer and more appropriate action being taken to resolve issues in the interests of both consumers and providers than where such information is lacking**.** As such we consider that the retention periods for all Relevant Data and Relevant DDRAC Data, to the extent that they comprise or include personal data, meet the necessity requirements of the storage and data minimisation principles.

Retention Periods for Relevant Data

10. All Relevant Data should be retained by all those involved in the provision of phone-paid services (network operators, Level 1 and Level 2 providers) for **two years as a minimum** from the point at which it is collected. This will ensure that valuable information is available for their own customer support purposes (particularly where complaints may not come to PSA's attention), as it will enable them to take action independently and monitor the effects of such action over a sufficient period of time. It will also ensure that such information is available for the PSA's regulatory purposes in all situations where they are likely to have significant value and subsequently be required.

11. Network operators and providers should ensure that Relevant data is flagged to ensure they are not purged in line with any set or triggered purge dates of the individual systems on which they are stored.

Retention Periods for Relevant DDRAC Data

12. All Relevant DDRAC Data should be retained by network operators and Level 1 providers for **three years as a minimum** from the point at which it is collected. The longer retention period for Relevant DDRAC data takes into account the fact that DDRAC concerns may, by their nature, emerge over a longer period of time. For example, where trends emerge which are suggestive of DDRAC failings at a higher point in the value chain (Level 1 providers and network operators) potentially in respect of multiple services or providers, or where there is a single or multiple underlying Level 2 provider Tribunal adjudication(s) pointing to a potential DDRAC failing higher up in the value chain. Such trends invariably take time to emerge, as would a Tribunal decision on the outcome of any complex investigation into an underlying Level 2 provider which points to DDRAC failures, and as a result increases the likelihood that a

DDRAC case would commence after a standard two-year retention period for Relevant Data has elapsed.

13. Network operators and providers should ensure that Relevant DDRAC data is flagged to ensure they are not purged in line with any set or triggered purge dates of the individual systems on which they are stored.

Retention Period for all Relevant Data and Relevant DDRAC Data where there is a PSA investigation

14. The PSA's experience is that its formal investigations can extend beyond the respective two- or three-years standard periods. This is particularly so in investigations relating to due diligence, risk assessment and control. It should also be noted that the technological landscape underpinning the premium rate services market is constantly changing and our investigations are consequently becoming more complex and in-depth. Such investigations necessitate more time for providers to supply evidence and responses to requests for information. It also necessitates more time for PSA to consider such responses, particularly where third party legal representation has been engaged, making the process more protracted.

15. We do not see this changing and it is vital that information is available throughout the lifespan of an investigation, even where the investigation is, necessarily, lengthy. It should be noted that the lengthier investigations are likely to be those carrying a larger number of associated complaints and/or a greater degree of alleged consumer harm or DDRAC failings. As such, where a case is allocated to one of the formal investigation tracks within either the two or three-year retention periods for Relevant Data and relevant DDRAC Data, **such data should continue to be retained by network operators and providers until advised by the PSA that the case or matter is closed.**

Non-exhaustive examples of specific types of Relevant Data and Relevant DDRAC Data

16. The Code currently requires providers to maintain various records (which are likely to include personal data) through the following provisions:

- Proof of Consent to Charge – paragraph 2.3.3
- Proof of Consent to Market – paragraph 2.4.2
- Evidence of Complaint Handling – paragraph 2.6.6
- Evidence of Due Diligence, Risk Assessment and Control on Clients – paragraph 3.3.1

17. Due to the changing nature of technology and market practice, PSA is unable to produce an exhaustive list encompassing all information that may be classed as relevant to the above. Providers should note this, and endeavour to identify and retain any sets of information which are not listed as examples below but may be of relevance to the provision and operation of phone-paid services and/or a PSA enquiry or investigation. This does not require networks or providers to actively collect and retain data which they would not be reasonably expected to collect.

18. While we have placed examples into various categories within the Relevant Data and Relevant DDRAC Data below this does not preclude an example of information in one

category being of relevance in other categories, or in relation to multiple code provisions. For example, transactional data may be relevant to proof of consent for charge or marketing but may also be tangentially relevant to other Code provisions, such as undue delay or a requirement for technical adequacy.

Relevant Data

Proof of Consent to Charging or Marketing

- Transaction logs, which includes all 3rd party data, including as appropriate…
    - Unique transaction IDs
    - Indication of whether transactions relate to a recurring subscription
    - Billing attempt status
    - IP addresses
    - MSISDNs or CLIs
    - User agent – e.g. Device make/model/build and Operating System used (including the version of the Operating System)
    - Dates/times of each component action – e.g. entry of MSISDN, sending of PIN loop message, entry of PIN loop message, pressing of initiation or confirmation buttons etc.
    - HTTP headers including non-standard X-header requests to URLs – such as "x-requested with…"
    - Timestamped records of the actual payment page served to the consumer, and its assets – e.g. images, CSS, Javascript etc.
    - Any Referrer URLs
    - Content of texts/emails
    - Call recordings
- Records of payment system alerts, and actions resulting from them
- Evidence of browsing, which includes all 3rd party data including….
    - HTTP headers including non-standard X-header requests to URLs – such as "x-requested with…"
    - Timestamped records of the coding behind served browsing pages
    - Timestamped screenshot records of served browsing pages together with the underlying HTML code and collateral which recreates it
- Evidence of consumer interaction with service, which includes all 3rd party data, including…
    - Timestamped logs of interactions, as per transaction logs above
    - Amount of bandwidth consumed by the consumer
- All URLs/domains used in promotions
- Keywords records from use of Direct Buy marketing (such as Google Adwords)
- Records of traffic split through affiliate networks
- Timestamped records of version changes to relevant webpages
- Records of print advertising
- Records of age verification checks
- Audio, Video and Images exchanged between the consumer and the service
- Records of STOP or other opt-out requests and actions
- Data around "churn" – i.e. opt-outs
- Bank statements
- Contracts
- Customer satisfaction survey data
- Records of MNO cards received
- Licences or agreements with commercial brands or other organisations
- Evidence of operator qualifications/experience

Complaint Handling

- Complaint data, which includes all 3rd party data, including…
    - Complaint figures relating to phone-paid services as received by L2s and L1s and Network operators
    - ”Trend” data (which is aggregated data that could indicate deviation from previous norms in relation to consumer behaviour), consumer complaints, or interaction with a website and/or payment mechanic
    - Data as a percentage of overall transactions
- All records of communication with consumers during the course of a complaint – email, paper, call recordings etc.
- Evidence of consumers requesting call recordings or transaction logs
- Refund policies
- Technical arrangements for refund platforms
- Evidence of refunds
- Refund “uptake” data

Other information

- As per paragraph 16 of this Guidance, networks and providers should endeavour to identify and retain any other sets of information that are not listed as examples above, but which may be of relevance to the provision and operation of phone-paid services and/or a PSA enquiry or investigation. This does not require networks or providers to actively collect and retain data which they would not be reasonably expected to collect.

Relevant DDRAC Data

- Records of and documents relating to Know Your Client or other due diligence checks undertaken
- Records of and documents relating to Risk Assessments and control measures
- Testing records and related documents – as well as records of any flags or unexpected discovery during testing, and subsequent actions
- Records of security alerts in systems, and any actions resulting from them
- Records relating to the resolution of all consumer enquiries and complaints relating to phone-paid services

Other information

- As per paragraph 16 of this Guidance, networks and providers should endeavour to identify and retain any DDRAC information that is not listed as an example above, but which may be of relevance to the provision and operation of phone-paid services and/or a PSA enquiry or investigation. This does not require networks or providers to actively collect and retain data which they would not be reasonably expected to collect.