Notice on Data Retention

Issued under paragraph 6.2.20 of the 15th Code of Practice (the Code)

This Notice is being issued to inform all providers of the types of information that are necessary to retain, and the time periods for which such information should be retained, in order to resolve consumer enquiries and complaints and enable effective supervision and/or engagement and enforcement.

In accordance with paragraph 6.2.21 of the Code any failure to comply with this data retention notice will constitute a breach of the Code.

Definitions of Relevant Data and Relevant DDRAC Data

1. For the purposes of the Code "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 the PSA during supervision or engagement and enforcement activities. "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 intermediary 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 any DDRAC supervision or engagement and enforcement activity.

2. Both Relevant Data and Relevant DDRAC Data may include personal data and may be requested by the PSA during a supervision activity or as part of an engagement and enforcement activity in relation to the promotion, operation, content or provision of a service, or when considering the due diligence and risk assessment undertaken by a network operator or intermediary provider in relation to their clients and/or services operated by them. The disclosure of such data is governed by law.

3. However, network operators, intermediary providers and merchant providers should note that this Notice sets out requirements 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 Notice 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, 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.

Disclosure and retention of personal data

4. This Notice is issued having full regard to the UK General Data Protection Regulation (GDPR), and the UK Data Protection Act 2018 (DPA) in respect of personal data.

5. UK data protection laws do not affect a phone-payment provider's ability to provide the 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.

6. In terms of further requirements under the first and other principles set out in the GDPR (fairness, transparency, purpose limitation), 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.

7. Where special categories of personal data are involved, consumers must give consent to such data being passed to the PSA (with providers expected to make all reasonable efforts to do so) unless another lawful basis under Article 9 of the GDPR applies.

8. 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 principle into account.

9. We consider that there is a clear need for PRS 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 effective PSA supervisory, engagement and enforcement processes that work in the interests of both providers and their consumers, ensuring that all relevant evidence is able to be considered.

10. 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 in the GDPR.

Retention periods for relevant data

11. All Relevant Data should be retained by all those involved in the provision of phone-paid services (network operators, intermediary providers and merchant 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.

12. Network operators, intermediary providers and merchant 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

13. All Relevant DDRAC Data should be retained by network operators and intermediary 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 (e.g., through supervision activities) which are suggestive of DDRAC failings at a higher point in the value chain (intermediary providers and network operators), potentially in respect of multiple services or providers, or where there is/are underlying merchant provider Tribunal adjudication(s), pointing to a potential DDRAC failing higher up in the value chain. The time it takes for such trends or concerns to emerge increases the likelihood that in some cases DDRAC engagement or enforcement activity would commence after the standard two-year period for Relevant Data has elapsed.

14. Network operators, intermediary providers and merchant 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 periods for all Relevant Data and Relevant DDRAC Data where there is PSA engagement or enforcement activity

15. Information must be available throughout the lifespan of any engagement or enforcement activity under section 5 of the Code. Throughout regulatory interaction for the avoidance of doubt where such activity commences during either the two or three year retention period for Relevant Data and Relevant DDRAC Data respectively **such data should continue to be retained by network operators and providers until advised otherwise by the PSA.**

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

16. The Code requires providers to collect, maintain or make available to the PSA various records (which may include personal data) through the following provisions:

- evidence of consumer consent to charges (paragraphs 3.3.14 - 3.3.17)
- evidence of consumer consent to be contacted (paragraph 3.6.2)
- information necessary to assist consumers in the resolution of their enquiries and complaints (paragraph 3.4.6)
- all documentation in relation to Due Diligence, Risk Assessment and Control (paragraph 3.9.15 and also paragraph 2.3 of Annex 2)
- results of intermediary provider platform security tests (paragraph 3.10.7).

17. Guidance on the Fairness Standard also suggests (in relation to the requirement at paragraph 3.3.5 of the Code) that records of consumer acknowledgement of excessive use warnings should be retained in a secure and tamper proof environment.

18. Due to the changing nature of technology and market practice, the PSA is unable to produce an exhaustive list encompassing all information that may be classed as relevant to the above. PRS 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 supervision, engagement or enforcement activity. This does not require such networks or providers to actively collect and retain data which they would not be reasonably expected to collect.

19. 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 evidence of consent to charge or marketing but may also be tangentially relevant to other Code Requirements, such as undue delay or technical standards.

Relevant Data

Proof of Consent to Charging or Marketing

- transaction logs, which includes all third-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, entry of account details and password, 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 third-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 third-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 mobile network operator cards received
- licences or agreements with commercial brands or other organisations
- evidence of operator qualifications/experience
- evidence of action taken and consumer acknowledgement of excessive use warnings.

Customer care

- complaint data, which includes all third-party data, including:
    - complaint figures relating to phone-paid services as received by merchants and intermediary providers 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
- evidence of individual consumers' consent to be contacted

- refund policies
- technical arrangements for refund platforms
- evidence of refunds
- refund "uptake" data

Other information

Networks, intermediary providers and merchant 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 PSA supervision, engagement or enforcement activity. This does not require such 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 activity undertaken in accordance with Annex 2 of the Code
- 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
- records of platform security checks undertaken in accordance with paragraph 3.10 (Systems Standard) of the Code

Other information

Networks and intermediary 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 PSA supervision, engagement or enforcement activity. This does not require networks or intermediary providers to actively collect and retain data which they would not be reasonably expected to collect.