PSA
Phone-paid Services Authority

Statement on PSA Guidance on the retention of data

19 September 2019

Contents

Executive summary

1. The Phone-paid Services Authority's (PSA) is the UK regulator for content, goods and services charged to a phone bill. Our vision is a healthy and innovative market in which consumers can charge content, goods and services to their phone bill with confidence.

   Our mission in the phone paid-services market is two-fold:

   - to protect consumers from harm
   - to further consumers' interests through encouraging competition, innovation and growth.

2. In light of the introduction of the EU General Data Protection Regulations (GDPR) into UK law, and the introduction of the Data Protection Act (DPA) 2018, the PSA decided to review its expectations as to the length of time for which providers would be expected to retain certain types of data, including personal data. Retention of data is necessary so that the PSA can request such data in the event of an investigation into the service or provider. The focus of the review was on providing industry with clarity around the data PSA expects to be retained, including personal data, and the retention periods that providers should apply to such data.

3. The PSA developed and consulted on a number of proposals in February 2019. In the consultation we summarised the proposals as the retention of all Relevant Data (including personal) for two years from the point at which it was first collected – with two exceptions: The first being that all relevant Data concerning providers' or networks' Due Diligence, Risk Assessment and Control (DDRAC) of a client or service should be retained for three years from the point at which it was first collected. The second being that where an investigation is opened during the two or three-year periods described above, all Relevant Data should be retained until such time that a provider or network is advised that the case or matter is closed. We also provided a list of non-exhaustive list of data that we considered to fall within Relevant Data and Relevant DDRAC data.

4. The consultation also made reference to earlier PSA publications which set out PSA's view as to how, for GDPR purposes, personal data could continue to be disclosed and retained lawfully

5. Following the consultation PSA received 4 responses from across the industry. Having fully considered the feedback we received, we do not see any reason to alter fundamentally the expectations we proposed on what types of data providers should retain as Relevant data or Relevant DDRAC data, nor the lengths of time they would be expected to retain it for. As such our original proposals remain the same in this respect. However, we have made some changes to the originally proposed guidance. These include:

   - Additional wording to paragraph 13 of the draft guidance to reflect an expectation that data is retained only where a provider could be reasonably expected to collect it.
   - Narrowed the scope of the term 'trend data' to clarify our intended meaning. Trend data is now defined as "aggregated data which would indicate deviation from previous norms in relation to consumer behaviour, consumer complaints, or interaction with a website and/or payment mechanic".

- A revision of the recommendation to keep timestamped screenshot records of served browsing pages. Following helpful feedback, we have now expanded this to include a requirement to retain both the screenshot and the underlying HTML code and collateral which recreates it.
- Simplification of some transaction log requirements by removing the references to "user-agent" and "referrer URLs" and replacing it with a requirement that all header information be recorded. We have also made explicit that HTML is an asset that should be retained in relation to the payment page.
- Outlined our expectation, following helpful feedback, that providers should ensure that Relevant data and Relevant DDRAC data is flagged to prevent them being purged in line with any triggered purge dates of the individual systems on which they are stored.

Background

About the changes to data protection law

6. In May 2018, two new pieces of legislation concerning the protection and processing of personal data came into force. The first was the EU General Data Protection Regulation 2016 (GDPR), the second was the UK Data Protection Act 2018 (DPA) which supplemented the GDPR and created exemptions from some of its requirements. Personal data is defined in the GDPR[1] as:

> *'any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;'*

7. The GDPR also set out a number of principles relating to the processing of personal data, which include the 'data minimisation'[2] and 'storage limitation'[3] principles. 'Lawfulness' is also a key part of the first principle set out in the GDPR[4] and the lawful bases for processing both personal data and special category personal data are also set out[5]. The DPA sets out various exemptions to other aspects of the first and other principles. PSA set out its views on the application of relevant principles, lawful bases and exemptions in its notice to industry in early 2018.

Previous PSA notice on the effect of the new data protection law

8. In March 2018, prior to the new legislation coming into force, PSA issued a Notice to industry. This Notice set out our current expectations around the retention and provision of data, including personal data as defined within GDPR, arising from specific rules in the PSA Code of Practice (the Code) and under directions for information made by PSA under the Code.

9. The Notice also set out the PSA's view that:

   - The new data protection laws would 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.

[1] Article 4(1) of Regulation (EU) 2016/679
[2] Article 5(1)(c).
[3] Article 5(1)(e).
[4] Article 5(1)(a).
[5] Articles 6 and 9.

- 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 PSA's opinion was that the requirements had not changed, and that consumers must give consent to such data being passed to the PSA (with providers expected to make all reasonable efforts to do so).

- 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[6], 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.

10. The Notice also outlined the PSA's intention to consult – as we have subsequently done – on revised expectations later in 2018.

[6] The PSA noted in the consultation that providers would need to undertake a legitimate interest assessment on each occasion. However, it is expected that it will be possible for providers to safely rely on this lawful basis in the majority of cases.

Consultation

Rationale for new expectations

11. The consultation which commenced on 6 February 2019 set out our expectations in relation to the retention of broader sets of information rather than just personal data. The overall aim was to help ensure that the PSA can adopt the right enforcement or other regulatory approach in addressing any identified harm or market issues. We proposed broader retention criteria, recognising that there are various types of information that are important and/or may be of strong evidential value to the PSA during an enquiry or investigation, whilst recognising that such information may be held by different parties involved in the provision of a phone-paid services. Our consultation also recognised that such data could also be useful to providers in understanding any consumer issues or complaints arising during the operation of their services, thereby enabling them to identify and resolve issues more quickly and effectively.

12. Our proposals, therefore, covered retention of broad sets of information, not just personal data. These were, in essence:

    - All information held by network operators and providers relating to the promotion, operation, content and provision of any premium rate service and any other information that may be of evidential value to an investigation ("Relevant Data").

    - 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 or operation of phone-paid services and/or of evidential value to a DDRAC investigation ("Relevant DDRAC Data").

Expectations

13. The consultation also set out the PSA's proposed expectations for the retention of data falling within the broad sets of information referred to above and relevant to the PSA's investigatory processes. These expectations were also set out in draft Guidance that was included in the consultation. The key proposals were:

    - Expectations in relation to retention of specific types of Relevant Data and Relevant DDRAC Data, including personal data, in particular:

        - Information which relates to proof of promotion and/or consent
        - Information which relates to the handling of consumer complaints and enquiries to a provider
        - Information which relates to the due diligence, risk assessment and control which the provider has carried out on parties with whom they contract

- Retention of all Relevant Data (including personal) for two years as standard from the point at which they are first collected, with the exception of information relating to due diligence, risk assessment and control ("DDRAC").
- Retention of all Relevant DDRAC Data which the provider holds on parties with whom they contract, for three years as standard from the point at which they are first collected.
- Retention of all Relevant Data where a PSA investigation is opened during the two- or three-year standard period, until such time that the provider or network is advised that the case or matter is closed.

Disclosure and retention of personal data

14. The consultation also reminded industry of the Notices that PSA had issued in March 2018 setting out its position in relation to the disclosure of information to PSA under both the GDPR and DPA. We made clear in the consultation that our position has, in essence, not changed from that referred to in the 'Previous PSA notice on the effect of new data protection law' section above.

15. We also made our view clear that the proposed retention periods for Relevant Data and Relevant DDRAC data would meet the *necessity* requirements of both the 'data minimisation' and 'storage limitation' principles set out in Article 5 of the GDPR. This is in essence due to the need for such information to be available for a sufficient period to enable an effective investigation by the PSA that works in the interests of both consumers and providers by ensuring that all relevant information and evidence is available to be considered.

16. We also identified the need for such information to enable providers to fully assist consumers in the resolution of their enquiries, including the provision of appropriate protection and redress for consumers where they have suffered harm or detriment as a result of phone-paid services.

Responses and considerations

17. The PSA consulted on its proposals regarding the retention of data, including personal data, on 6th February 2019. The consultation concluded on 3rd April 2019. During this time, the PSA received four responses to the consultation. One of the respondents requested that both their identity and their response should be kept confidential. Our consideration of those responses, and our determination in respect of them, is as follows.

Expectations in relation to retention of specific types of Relevant Data and Relevant DDRAC Data.

Q1. Do you agree with the non-exhaustive data sets listed within Annex A? If there is anything that you consider should be added to, or removed from, the list please explain why.

18. Some respondents said that they do not keep, nor would have reason to keep, some of the data listed in the proposed Guidance. They asked for clarity that they would not be expected to collect and retain all the datasets outlined in the proposed Guidance, regardless of whether they are actually capable of collecting it in the first place.

19. We acknowledge that some parties in a value chain will not have the ability or any reason to keep all of the data we have listed with the Relevant Data and Relevant DDRAC data categories. For example, a Level 1 operating a payment platform will retain data which the Level 2 merchant involved in the same transactions will not or may not even have access to. As such, we have added wording around paragraph 17 of the draft Guidance to reflect an expectation that data is retained only where the provider could be reasonably expected to collect it and has collected it.

20. One respondent also stated that they use the data minimisation Principle and, as such, holding data in case of a request from the PSA would not be consistent. We do not agree that the holding of data for the purposes we have set out is inconsistent with the data minimisation principle. We have already made reference to the requirement of *necessity* and how, in our view, our proposals meet this test.

21. We, of course, recognise that, in practice, it will be for each provider, as data controllers, to ensure that they comply with the GDPR in relation to any personal data they process. However, we do not agree that our general expectations are inconsistent with or will, in general, cause providers to fall foul of the relevant GDPR principles. Furthermore, where providers are in doubt in respect of particular data sets, they will be able to seek further advice from the Information Commissioner's Office.

22. In any event, as we have already stated, our proposals were not limited to personal data but included broader data sets which are not subject to GDPR.

23. One respondent asked for clarification on what was meant by "trend data". We had used the term "trend data" to describe any aggregation of incidents such as consumer complaints, attempted or successful attacks on a providers' system, specific flags which a platform would raise in relation to attempted or successful attacks, and other such data which would indicate a

rise or fall in the previous norm. However, we recognise that "trend data" can have a meaning that goes beyond this specific and narrow scope. As such we will drop the use of this term from the final version of the Guidance. Instead we will use "aggregated data which would indicate deviation from previous norms in relation to consumer behaviour; consumer complaints, or interaction with a website and/or payment mechanic". The final Guidance has been altered accordingly.

24. One respondent suggested that there was no need to keep timestamped screenshot records of served browsing pages. Instead, what would be relevant was the HTML code and collateral sent to the consumers' device. Having considered this further, we accept that the screenshots generated by the L1 or L2 provider are generally programmatically recreated by a script that uses the html, CSS and other page assets to recreate a rough representation of how the page would have been displayed to the user. As such, we are altering the Guidance to reflect an expectation that providers should retain both the screenshot and the underlying script which recreates it.

Retention of all Relevant Data for two years as standard

Q2. Do you agree that two years is an appropriate period for all Relevant Data to be retained as standard, to enable sufficient time for (i) commencement and progression of PSA enquiries and determination of appropriate action and (ii) resolution of complaints and/or concerns by network operators and providers? If not, why not?

25. One respondent asked if we could add a caveat referencing the fact that other legal retention periods exist alongside the PSA requirements. We recognise there are other legal requirements that may apply, but the focus of our document is to set out our expectations. As such, we do not consider that there is a need to reference such other requirements.

26. One respondent questioned why retention of data was necessary, given their belief that evidence could be preserved at any stage by the PSA initiating an investigation. It would clearly be unlawful for the PSA to initiate a formal investigation solely for the purpose of securing or preserving evidence and we would never seek to do so. There are clear tests set out in the Code, as well as legal principles that apply in relation to the commencement of enforcement activity. As such, our view remains that it is necessary for the PSA to set out its expectations in relation to the retention of such data and for providers to be able to consider how they meet the expectations whilst complying with the GDPR and DPA.

27. One respondent argued that holding personal data unnecessarily causes consumer harm in and of itself. They also made reference to the Limitation Act 1980, which sets the ordinary time limit for contract disputes at 6 years, and stated that it would ordinarily motivate a provider to maintain proof of consent to charge from the last instance of that successful charge. However, with the coming into force of the GDPR, the fact that the sums involved are small and the industry is sufficiently well regulated, providers can rely on a reasonableness/balance of probabilities defence. They go on further to argue that, where a consent to charge process is flawed, this would be discovered early. As such, they argued that because the PSA had not mentioned "accrual of cause" in the consultation, that if a consumer had joined a subscription

service in 2017, had not stopped that service and was still being billed and no PSA investigation commenced, then they would be free to delete the evidence of consent to charge. The respondent goes on to argue that only more recent evidence of non-compliance is relevant to PSA and any loss of earlier evidence should not be material, as PSA investigates the service and not the experience of individuals. The respondent also argues that in any event a two-year retention period is too long and that one year is sufficient.

28. We fundamentally disagree with these arguments.

29. Firstly, the premise of the Limitation Act in relation to contracts is irrelevant to the regulation and enforcement of phone-paid services. Contractual disputes are clearly and materially different to non-compliance with the law or rules and regulations produced and issued under power of the law (such as the PSA Code of Practice). Evidence of non-compliance with rules set under the Code are not time limited and can and should be considered in each case. The PSA, of course, always remains under a duty to ensure that it is fair and proportionate in its conduct of investigations, which includes its consideration of relevant evidence.

30. Secondly, evidence of non-compliance clearly goes towards consideration of the seriousness of any breaches of the Code and harm occasioned to consumers, which in turn informs the sanctions that are appropriate for the non-compliance. The fact that knowledge of the occurrence of any non-compliance or harm has not yet reached the PSA enabling it to investigate does not alter this. Furthermore, consumers who have been subject to harm for a long period of time (e.g. because they had not knowingly subscribed and had not, for example, noticed small and consistent charges on their bill over several months or even years) would rightly expect the PSA to consider all evidence relating to the entire period of their harm rather than the last instance of it.

31. For these reasons, we do not agree that the provision of consent to charge or other information should be limited to the last 'accrual of cause' or instance of non-compliance.

32. One respondent suggested that there were several providers who would find our requirements to be in conflict with their existing contractual arrangements. Where this is the case, we would expect the existing arrangements to be changed, to enable providers to come into line with the expectations set out in the Guidance. We see no reason to alter the expectation for all Relevant data (as is applicable) to be retained for 2 years for this reason.

33. However, in some cases the opposite was true, and respondents highlighted that existing contractual arrangements for data retention were, in fact, more onerous. Where existing contracts already go beyond the expectations set out in the Guidance, the PSA sees no reason why they should not continue as they are. The decision to continue to do so will remain with the relevant providers.

34. Several providers requested confirmation that, should a data subject ask to be forgotten, the PSA expectations on standard retention of data will take precedence. Since the PSA is not the data controller in respect of any personal data held by a provider, it is unable to provide such a confirmation. As data controllers, providers will need to carry out their own assessment with

reference to the GDPR[7], with reference to our Guidance, in the event that such a request is received from a consumer.

Retention of all Relevant DDRAC Data for three years as standard.

Q3. Do you agree that three years is an appropriate period for all Relevant DDRAC Data to be retained as standard, so as to enable sufficient time for (i) commencement and progression of PSA enquiries relating to DDRAC and determination of appropriate action and (ii) resolution of concerns by Level 1 providers and network operators? If not, why not?

35. One respondent suggested that many within the industry already hold DDRAC data for three years. As such, and in light of there being no responses to Q3 which disagreed with our proposal in respect of Q3, we will retain the expectation for providers to retain all Relevant DDRAC data (as is applicable) for three years as proposed.

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

Q4. Do you agree that all Relevant Data and Relevant DDRAC Data should be retained throughout the lifespan of an investigation? If not, why not?

36. One respondent pointed out that Relevant data and Relevant DDRAC data will often be spread over several storage locations. As such, this data would need to be flagged to ensure it was not purged in line with the purge dates triggered by individual storage systems. We note this and have added an expectation to the Guidance to ensure that Relevant data and Relevant DDRAC data must be flagged to ensure they are not purged in line with any triggered purge dates of the individual systems on which they are stored.

37. Two respondents expressed a concern that there appears to be no limit on the time that an investigation could take. One respondent stated a belief that Question 4 related to the period the PSA had for "discovery", and expressed a view that a "discovery" period should not continue indefinitely because investigations stayed open for a prolonged period. They also suggested that the PSA was free to keep its own copy of evidence which a provider had previously passed to it even after a provider has deleted the same data.

38. We believe this view to be mistaken. The PSA does not operate investigations under a "discovery" process. Information relevant to an enquiry or investigation is requested at the point at which such information is required. The PSA does not seek (or discover) information held by a provider over a continuous period of time. In the PSA's view, retention of data is not the same as "discovery".

39. In any event, the principle of proportionality means that information requests that we make must be proportionate to the nature of the investigation or enquiry being conducted and, therefore, not everything held by a provider would be sought by the PSA. Our proposals, therefore, do not relate to "discovery" but, rather, the need to ensure that all relevant

[7] Providers will need to consider Article 17 in particular, and whether any of the conditions in paragraph 2 are met to enable erasure, or a paragraph 3 exclusion applies.

information (which then enables PSA to request only those that are required for a specific enquiry or investigation) is available in the event of, and for the duration of, an enquiry or investigation.

40. As such, the PSA will ask for information as it becomes relevant for an enquiry or during an investigation. Furthermore, we would not regard relevant data as being "spent", and the provider's obligation to retain it discharged, after a first request for information or data where an investigation has not concluded. This is because, during an investigation, the PSA may need to request further information as a result of information it has received from a provider in response to a previous information request, or further information received from consumers, or as a result of (further) monitoring by PSA.

41. Therefore, we will retain our proposed expectation for all Relevant data and Relevant DDRAC data (as is applicable) to be retained throughout the lifespan of an investigation. We can confirm that the PSA will always progress investigations as expeditiously as possible. Whilst we cannot set defined boundaries as to the length of any investigation, we would expect formal investigations lasting longer than two years to be exceptional.

Personal Data – GDPR considerations.

Q5. Do you agree with our assessment in relation to the GDPR considerations? Is there anything else in terms of GDPR that we should take into account?

42. One respondent expressed the view that it should not be the responsibility of a provider to retain the promotion which a consumer saw. If the consumer believes they were misled by the pre-purchase information, then they should evidence it themselves. We do not agree that the burden of retaining and evidencing promotions should fall to consumers. A promotion is instrumental in a consumer making a decision to purchase a service or not, and our Code requires that such promotions present all key information clearly, and do not mislead. The relevant Code provisions are a responsibility that falls on providers, and so the responsibility for providing evidence that they have complied with Code requirements should rest with them.

43. One respondent, a trade association, said that a number of their members had requested clarity over retention of any data which is transferred to a different person when a mobile device is sold or given to a new owner. Examples would be phone numbers, the IMEI and IMSI numbers ascribed from the actual device, and IP address data from where the handset has browsed the web.

44. It is not immediately clear to the PSA how a provider would identify if a handset had been sold or given to a new owner, short of the owner actually contacting the provider to inform them - an action we would consider very unusual. However, the services and the data associated with the mobile number for the period that the services are consumed remain relevant, regardless of whether the handset or number has been transferred to a new owner in the interim. As such our view remains that any data which relates to the service operation (for example promotional and transactional data) and also to the device on which it was carried out should

be retained.

45. A similar question was asked around the retention of data where an existing service is transferred from one payment aggregators' platform to another aggregator's platform. We can confirm that in the event of a service being transferred between two aggregators, the original aggregator should retain all Relevant data and Relevant DDRAC data (as is applicable) relating to the service whilst it operated on their platform. The subsequent aggregator will also need to retain such data relating to the service from the point at which it becomes operational on their platform.

46. Lastly one respondent asked what would happen in the event that a consumer specifically exercised their right under GDPR to be forgotten and to have their data deleted. We have already addressed this issue at paragraph 34 above. We would add that, where a provider, having carried out the necessary assessment in relation to the request for erasure, decides that it is appropriate to comply with it, they should ensure that this decision is recorded in line with any guidance issued by the ICO from time to time. Providers should note that if a consumer subsequently advises the PSA that no request for erasure was made to the provider, this would be a relevant factor for a Tribunal to take into account in considering whether information ought to have been available when requested by the PSA. Having a proper record of the assessment and decision should assist providers in this respect.

Q6. Having considered the proposals in this consultation do you agree with the proposed Guidance at Annex A of this document? If not, why not?

Impact Assessment

47. Several respondents expressed concern over the logistical impact of retaining all data for the lifespan of an investigation. Some asked that the PSA consider additional costs to those in their impact assessment, that go beyond hardware, such as additional administration and supervision costs.

48. One respondent highlighted a number of industry members who were concerned that the requirements set out should not be applied retrospectively, in order that the industry could deliver more effectively.

49. We acknowledge that the impact of retaining the proposed data will fall differently on different providers, dependent on the current sets of data which they retain and the way in which they currently retain them. We do, however, note the following:

    - It is in a provider's interest to ensure that it is able to respond fully to any request from the PSA during an investigation, the benefit being that this would enable the PSA to reach appropriate and proportionate decisions in relation to investigations (such as whether or not to investigate formally and if so what track to use, and determine whether any apparent breaches fall away or should be withdrawn) and adjudications by a PSA Tribunal (as to whether or not sanctions are required, or the level of such sanctions).

- Retention of data as proposed will also be useful to providers in understanding any consumer issues or complaints arising during the operation of their services, thereby enabling them to identify and resolve issues more quickly and effectively.

- We have already set out above the objectives and benefits of the proposals for PSA's investigatory and enforcement activities. This also carries significant benefits for consumers in that where there is a finding that non-compliance has led to financial harm a PSA Tribunal will (where appropriate), with the benefit of retained relevant data before it, be able to order refunds covering a greater period of the harm occasioned.

- The GDPR Notice to Industry, published in March 2018, put industry on notice of the PSA's intention to consult on data retention periods. As such, providers have had a considerable period of time to consider their data retention periods more generally and plan for potential changes in our regulatory expectations, including whether or not it necessitated any further administration or supervision requirements.

50. With regard to the question of retrospective application of the Guidance we cannot see how an expectation to maintain all Relevant data and Relevant DDRAC data aids more effective delivery where it only applies to data being collected from the date at which the Guidance comes into force. In any event, such data will already be held by various providers and it is not our intention to suggest that the data can or should be deleted or, indeed, encourage such deletion. We have, therefore, made clear in the Guidance that it also applies to all Relevant data and Relevant DDRAC data that is being held as at the date of the Guidance coming into force notwithstanding that such data was collected prior to the Guidance.

51. We have taken the opportunity to amend the first sub-bullet of the 'Complaint handling' section in the 'Relevant Data' list in the Guidance to include complaints figures received from network operators, and to clarify that the figures referred to are those relating to phone-paid services. This is a minor change and although not included in the draft Guidance does not, in our view, create any additional or distinct impact in respect of the proposals. The text of the sub-bullet now reads: '*Complaint figures relating to phone-paid services as received by L2s and L1s and network operators*'.

52. Finally, we have simplified some transaction log requirements within the Relevant Data list by removing the references to "user-agent" and "referrer URLs" and replacing them with a requirement that all header information be recorded. We have also made clear that HTML is an asset that should be retained in relation to the payment page. Again, these minor changes do not in our view create any additional or distinct impact in respect of the proposals.

53. Having considered the responses to Question 6 and our impact assessment, we do not consider that the impact of our proposals is disproportionate to their objectives such as to lead us to conclude that we should not proceed with them.

54. In developing this Statement, the PSA has considered the feedback and input received from the 4 responses received to the consultation, and other more general or informal feedback given to us.

55. The list of stakeholders who responded to the consultation and indicated that they were happy for their responses to be published are as follows (in alphabetical order):

    - Aimm
    - Anonymous respondent
    - Infomedia Services Ltd.
    - Safari Mobile (UK) Ltd.

Next steps and implementation

56. Following this consultation, and our consideration of all responses received, PSA will be implementing the proposed Guidance on the Retention of Data with the revisions made as advised within this statement.

57. The PSA has determined that the Guidance should take effect immediately, as there are a number of network operators and providers that are already holding various Relevant data and Relevant DDRAC data, and some are doing so fully in line with our expectations, albeit under their individual contracts or policies. As such, we consider that it is both reasonable and appropriate to expect retention of such data to continue in line with our expectations.

58. We note that there may be providers that are not yet retaining some of the Relevant data or Relevant DDRAC data that they collect in line with our expectations, including retaining data for the expected duration(s). Therefore, and in line with our impact assessment response above, we will allow a period of up to six weeks to enable such network operators and providers time to come into line with our expectations before we consider the need for any enforcement action. Our expectation is therefore that such network operators and providers come into line at the earliest point possible during the six-week period rather than simply taking advantage of the entire period.

59. The revised Guidance is provided below, as an Annex to this statement. The changes made to the Guidance following consultation are highlighted in yellow for ease of reference. The Guidance will take effect on the date of publication.

ANNEX A

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 collected 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 is held by network operators and providers as at the date of this Guidance coming into force as well as such data collected after this date.

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[8]. 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[9], focussing on the legitimate interests of the provider

[8] The full version of this Notice is available here.
[9] The PSA notes that providers would need to undertake a legitimate interest assessment on each occasion. However, it is expected that it will be possible for providers to safely rely on this lawful basis in the majority of cases.

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…"~~ HTTP request and response headers sent to and from the client - e.g. User agent, Referrer, Cookie etc. Custom propriety headers should also be included - e.g. "X-Requested-With"
    - Timestamped records of the actual payment page served to the consumer, and its assets – e.g. ~~images,~~ HTML, CSS, JavaScript, images 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…"~~ HTTP request and response headers sent to and from the client - e.g. User agent, Referrer, Cookie etc. Custom propriety headers should also be included - e.g. "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 Ads ~~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 17 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 17 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.