PSA
Phone-paid Services Authority

Consultation on PSA Guidance on the retention of data

6 February 2019

The UK regulator for content, goods and services charged to a phone bill

Contents

Executive summary

The Phone-paid Services Authority (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 market is:

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

In this consultation, we put forward proposals to clarify the PSA's expectations as to how long providers will retain certain types of Relevant Data, including personal data, so that the PSA can request such data in the event of an investigation into the service or provider. This is in light of changes in May 2018 to UK legislation concerning the protection and processing of personal data.

The proposals can be summarised as the retention of all Relevant Data (including personal) for two years from the point at which it was first collected.

This is 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 exception is 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.

These proposals are set out in the consultation, and the Guidance on which we are consulting, at Annex A. For further clarity, Annex A to the document also sets out a non-exhaustive list of data which the PSA considers relevant.

Background

About the changes to data protection law

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 supplements the GDPR and creates exemptions from some of its requirements. Both laws cover personal data, which includes any information that an individual can be identified, directly or indirectly, from.

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

In March 2018 the PSA issued a Notice, ahead of the arrival into force of the new legislation. This Notice sets out our current expectations around the retention and provision of data, including personal data, arising from specific rules in the PSA Code of Practice (the Code) and under directions for information made by the PSA under the Code.

The Notice also sets 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.*

- 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[1], focussing on the legitimate interests of the provider and/or their consumers. Providers duly relying on the "legitimate interests" basis

[1]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.

would not need to seek the consent of individual consumers before providing their data to the PSA.

PSA's view, as set out in the previous Notice, was that all data in relation to phone-paid services accounts and transactions should be retained for a minimum of two years from collection. The previous Notice also outlined the PSA's intention to consult on new proposed expectations later in 2018.

Rationale for new expectations

While the changes to data protection law have precipitated the Notice and necessitated consultation on guidance in relation to retention of personal data, the PSA considers it necessary to consult on its 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. We believe a consultation on retention of broader information is necessary because there are other types of information that are important and/or may be of strong evidential value to the PSA during an enquiry or investigation, helping to ensure that the PSA is able to adopt the right approach in addressing any identified harm or market issues.

However, where information (including personal data) that would likely assist PSA during an investigation is no longer available at the point at which a provider is requested to provide it, this has the effect of hampering PSA's understanding and evidencing of issues that may have affected consumers of the service. Better, or more comprehensive, retention and analysis of information retained may also assist providers in understanding any consumer issues or complaints that come to light during the operation of a service, enabling them to identify and resolve issues more effectively.

The proposed Guidance therefore covers retention of broader sets of information, not just personal data. In essence, these are:

- 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").

See draft Guidance at Annex A in this document for a non-exhaustive list of Relevant Data and Relevant DDRAC Data compiled by the PSA.

Proposals

We are consulting on Guidance which sets out new expectations for the retention of data relevant to our investigatory processes (see draft Guidance at Annex A in this document). The key proposals within the draft Guidance are:

- 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.

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

In considering the specific types of information which the PSA expects providers to retain, we have started by considering the types of information that we are aware of that may be relevant to the promotion, content, provision or operation of phone-paid services and/or provide useful evidential value to PSA during an enquiry or investigation.

We have also considered specific provisions of the Code that require retention of evidence and/or documentation. This has allowed us to formulate a non-exhaustive list, within the draft Guidance attached at Annex A, of specific types of information that we propose providers should retain.

Information listed within draft Guidance at Annex A which are, or are likely to include, personal data are set out and considered in more detail in the 'Personal Data – GDPR Considerations' section below.

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.

Retention of all Relevant Data for two years as standard

The PSA proposes that 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 they are collected. This ensures that valuable information will be available for the PSA's regulatory purposes in all situations where they are likely to have significant value and may subsequently be required.

We believe that network operators and providers may also consider such retention to be necessary for their own customer support purposes (particularly where complaints may not come to PSA's attention), as it enables them to take action independently and monitor the effects of such action over a sufficient period of time.

While the PSA endeavours to commence enquiries and investigations as quickly as possible, there are circumstances which either individually or cumulatively could extend this and/or necessitate the initial requesting of information at a much later point than normal. Examples would include, but not be limited to:

- Where there are initial concerns about a service or provider, but these do not result in a decision at that point to allocate the matter to an investigation track under the Code but subsequently further concerns about the service or provider call for further enquiries at a later stage.
- Where complaints about multiple services at different times lead PSA to request such information to assess the compliance of a payment platform or promotional mechanic over an extended period of time.
- Where a provider fails or refuses to provide some or all information which the PSA has requested at the enquiry stage and delay is caused as a result.
- Where the value chain for the provision of a phone-paid service is unusually complex, requiring the PSA to first establish the roles of each party within the chain before requesting information from them.

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?

Retention of all Relevant DDRAC Data for three years as standard

The PSA proposes a longer retention period, three years as standard, for Relevant DDRAC Data. In doing so we have taken 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 DDRAC failings higher up in the value chain become apparent following a single or multiple underlying Level 2 provider Tribunal adjudication(s). Such trends may take some 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 elsewhere in the value chain. As a result, this increases the likelihood that a DDRAC case would start after a standard two-year retention period for Relevant Data has elapsed.

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?

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

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.

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. As such, we are proposing that where a case is allocated (within the respective two or three-year retention periods proposed above) to one of the formal investigation tracks, all Relevant Data or Relevant DDRAC Data should continue to be retained by network operators and providers until advised by the PSA that the case or matter is closed.

We consider this necessary to ensure that we can perform our duty as a regulator, carry out investigations and protect consumers where appropriate. It is important to note 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.

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

Personal data – GDPR considerations

We have considered whether our proposed retention periods accord with the obligations on data controllers under the GDPR in respect of personal data. In particular, the requirement for necessity in relation to the storage limitation and data minimisation principles. We have assessed these specific obligations and balanced them with the need to ensure that providers retain the necessary information for a sufficient period to fully assist consumers in the resolution of their enquiries and complaints - 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.

Where all relevant evidence can be considered, this 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 proposed retention periods meet the necessity requirements of the storage and data minimisation principles. Paragraphs 22 to 30 below provide more details on why PSA considers it necessary for network operators and/or providers to retain relevant personal data, particularly for investigatory purposes.

We have identified the following data sets (from both the Relevant Data and Relevant DDRAC Data categories) as being likely to contain personal data:

a) Content of texts or emails – either those which have been sent by the consumer, or those sent from a service to a consumer, which may contain the consumer's name or other personal details.
b) Call recordings.
c) Evidence of operator qualifications/experience – where an operator provides specialist advice which would require such qualifications or experience under our regulation.
d) All records of communication between any party in a value chain and a consumer during the course of a complaint
e) Evidence of consumers requesting call recordings, transaction logs, or other evidence of interaction with a service
f) Evidence of refunds or refund uptake data (where a consumer has provided personal data such as address or bank account)
g) Records of Know Your Client checks, including identification records
h) Bank statements – which may contain personal details where a provider is a sole trader
i) Contracts – which may also contain personal details, e.g. where a provider is a sole trader
j) All records of consumer interaction with a service – this would include:
    - MSISDNs and CLIs (i.e. mobile and "fixed" phone numbers)
    - X-header requests to URLs – i.e. where a mobile device makes a request to be served with a specific webpage
    - Timestamped evidence of consumer interactions with a service
    - Records of age verification checks performed against a consumer's MSISDN

With respect to a) and b), the retention of this information allows the PSA to analyse the nature of interactions that the consumer has had with operators (or chatbots). This is essential to determine various matters during an investigation. For example, whether a consumer has received the correct information before agreeing to a purchase or a charged onward connection, whether a consumer has been delivered a different service from the one which they were led to believe they would receive, or whether a provider has facilitated underage access to services with adult content.

With respect to c), the PSA has long-standing rules which require certain types of counselling or advice services to use only appropriately qualified operators[2]. In addition to the general

[2] The link to these requirements on our website can be accessed at https://psauthority.org.uk/for-business/-/media/Files/PSA/For-Businesses/Guidance-and-compliance/Explore-our-

reasons we have outlined in paragraph 143, we also consider that the effects of advice or counselling given by someone who was not properly qualified for the role may not be immediately apparent. It is essential that providers retain evidence of the experience and qualifications of any such employees, even after they have left their employment, otherwise it could have a serious impact on the quality and effectiveness of any later investigation into, for example, a service involving an operator who was alleged to have given bad advice or counselling.

Regarding bullets d) and e), we note that consumers may make complaints to a provider before they first contact us. Consumers should not be expected to retain their correspondence with a provider or their requests for information, or any information such as that which they have submitted in a complaint form or during an exchange with a chat bot. We believe it is likely, where a complaint to a provider remains unresolved for a considerable period, that such correspondence or requests will be lost or deleted. We consider it to be the responsibility of providers to retain such information.

In considering f), we note that evidence of refunds will often be important mitigating evidence, relevant to the sanctioning process where alleged breaches are upheld. Evidence relevant to sanctions will, by its nature, be required at the very end of the enforcement process.

Concerning g), it is not uncommon for parties within the value chain to have contractual relationships, especially between aggregators and merchants, which go back for a significant number of years. Should an investigation, or number of separate investigations arise, which bring into question the Due Diligence performed on a client, it would be necessary to analyse the most recent Know Your Client checks which a provider has performed. It is sometimes the case that parties do not renew KYC checks for several years once they are first completed, especially if ongoing Due Diligence has not identified any risk in the intervening time.

In respect of h) and i), we note that providers would be required by other legislation to retain financial and contractual records for at least seven years, so we do not consider our requirement to have any disproportionate impact in terms of GDPR.

Lastly, in relation to j) the PSA considers retention of records which are linked to MSISDNs and/or CLIs to be extremely important in the great majority of investigations it conducts. This is because they are the primary method by which consent to payment and interaction (both pre and post-purchase) can be linked back to a consumer who complains in respect of a phone-paid service and/or age verification checks for that consumer can be confirmed. Because a variety of different parties in the value chain will hold records of interaction or consent to purchase which are linked to a MSISDN or CLI, those numbers perform a useful function in allowing the PSA to clearly check whether there are any inconsistencies between records of the same purchase or interaction which exist on different platforms.

There are a number of factors which can delay either the start of an investigation or an investigation itself while it is in progress. If data which links to or references a MSISDN or CLI has been removed from records by that point, then the PSA would effectively be unable to

---

guidance/Guidance-files/27_Notice-of-SC-for-Professional-services.ashx?la=en&hash=BB83AF32224095915D41099A022893BAC481DFCE

investigate a consumer's allegations. The PSA is aware of several situations where, after a period of time has elapsed, providers have not retained data which would otherwise be useful during an investigation. This has reduced the evidence available and we are keen to ensure that this does not affect our ability to address consumer harm effectively moving forward.

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?

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

In considering retention of all Relevant Data for two years and Relevant DDRAC Data for three years as standard, as well as retention until closure where a case has been allocated for a formal investigation, the PSA has considered the general impact of such retentions , including any impact that may be caused by the need to store data (including personal data).

We consider the main impact will be in terms of storage costs where providers do not currently store some of the data sets specified in the non-exhaustive lists within the draft Guidance at Annex A. This would be especially relevant to the storage of browsing pages as served to a consumer, and the records of the coding behind them, as in our view they are likely to require the greatest storage capacity out of all the data outlined.

However, we consider the storage of data to be a negligible cost. Server arrays in a digital enterprise environment would usually "stripe" data across 3-5 disks in order to provide fault tolerance (i.e. if one disk stops working, the others can assume the broken disk's work and recover most of the data). The cost of one terabyte of data storage in this environment is currently between £150 and £700, which when multiplied by 3 or 5 raises the estimated maximum cost to between £2100 and £3500. While there may be similar additional costs in terms of purchasing additional equipment to house data disks, set them up into new arrays, and join them to existing infrastructure, we do not consider the total cost to be significant. As such, we do not envisage that the need to store data for three years (in some circumstances) as opposed to two will carry a significant cost impact on phone-paid providers.

We note that the ICO's guidance on GDPR suggests that the risk of storing rather than deleting personal data is significantly reduced where storage is offline, thus reducing the risk of mistakes or misuse. We see no reason why information, including personal data, should not be stored offline. While this may create some extra staff resource in terms of information retrieval, we would consider this to be proportionate when set against the need to ensure consumer complaints can be resolved and investigated where required.

We would welcome any views that respondents have on the practicality of storing personal data offline and retrieving it in response to a PSA request.

Consultation questions and how to respond

We welcome responses to the questions posed above, along with any views respondents may have relating to our ongoing considerations around data retention. The questions posed are repeated here for ease of reference:

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

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 providers? If not, why not?

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?

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

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?

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?

We plan to publish the outcome of this consultation and to make available all responses received. If you want all, or part, of your submission to remain confidential, please clearly identify where this applies along with your reasons for doing so.

The closing date for responses is 3rd April 2019.
Where possible, comments should be submitted in writing and sent by email to consultations@psauthority.org.uk

Copies may also be sent by post to:

Kelly German
Phone-paid Services Authority, 25th Floor, 40 Bank Street, London, E14 5NR

Personal data, such as your name and contact details, that you give to the Phone-paid Services Authority will be used, shared, stored and otherwise processed, so that the PSA can obtain opinions of members of the public and representatives of organisations or companies about the PSA's proposals regarding the retention of data and records and publish anonymised findings. Further information about the personal data you give to the PSA, including who to complain to, can be found at psauthority.org.uk/privacy-policy.

If you have any queries about this consultation, please email using the above contact details.

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 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.

Disclosure and retention of personal data

4. 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).

5. 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.

6. 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

[3] The full version of this Notice can be accessed at - https://psauthority.org.uk/for-business/~/link.aspx?_id=28F062A61EA84FEABB72B55836FB3E70&_z=z

[4]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.

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.

7. 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.

8. 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

9. 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.

Retention Periods for Relevant DDRAC Data

10. 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.

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

11. 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.

12. 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

13. 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

14. Due to the changing nature of technology and market practice, PSA is unable to produce an exhaustive list, which encompasses all information which 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.

15. 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
- 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 as received by L2s and L1s

    - Trend data
    - 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

- Any other information that may be relevant to the provision or operation of phone-paid services and/or of evidential value to PSA during an enquiry or investigation; for example, where possible copies of digital or other content provided to consumers.

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
- Any other information that may be relevant to the provision or operation of phone-paid services by network operators and their contracted parties and/or of evidential value to a PSA enquiry or investigation