

# aimm response to the PSA Guidance on the Retention of Data Consultation

Prepared by Joanna Cox, General Manager, aimm on behalf of the aimm membership

## Introduction to aimm

The Association for Interactive Media and Micropayments (aimm) is the specialist UK-based trade organisation representing the commercial and regulatory interests of member companies involved in the interactive media and micropayment industries - where consumers interact or engage with services across converged media platforms and may pay for those services or content using a variety of micropayment technologies including premium rate. We are a not for profit organisation, funded by our members, run for our members. We create conditions for growth and protect the regulatory environment in which our members operate.

aimm has a membership that represents the entire value chain - from the providers and promoters of services and content to the network operators and technical service providers that deliver and bill them to customers. No other organisation has such reach or representation. Members of aimm work collaboratively to address key industry issues and to build a trusted business environment, encouraging investment, creating new opportunities and developing business partnerships.

We uphold our Code of Ethics and Core Values to create an environment of consumer trust and industry confidence within which our members' commerce can grow. We will facilitate communication and engagement throughout the value chain to ensure a coordinated industry approach to excellence and success in interactive services.

We are committed to furthering the interests of Interactive Media and Micropayments through the regular exchange of information and communication throughout the value chain, effective engagement with regulators and legislators and the presentation of a successful industry image to consumer and business media.

aimm promotes excellence in the world of interactive media and micropayments. The purpose of aimm is to create an environment of consumer confidence and trust within which our members' commerce can flourish. aimm promotes and abides by the philosophy that consumers who are accurately and openly informed of the nature, content and cost of participation in an interactive service experience should be perfectly placed to exercise their freedom of choice and thereby enjoy the most effective form of consumer protection.

creating the conditions for growth in micropayments

## Membership input

aimm welcomes the opportunity to respond to the Phone-paid Services Authority (PSA) Guidance on the Retention of Data Consultation. To assist aimm in providing a comprehensive input to the Phone-paid Services Authority, aimm communicated with its Members in the following manner;

- Written input from Members
- One-to-one discussions in person and over the telephone

aimm Members who operate in the Phone Paid Services markets are broadly split into seven categories although there is some overlap inside individual Member businesses.

- Fixed Line Networks who are often Fixed line L1
- Mobile Networks
- Mobile L1 aggregators
- L2 providers of traditional PRS services (fixed line, PSMS, and DCB)
- Broadcasters (who are often L2 providers)
- Charities and Charity enablers (who are often L2 providers)
- Industry Support companies

aimm sought responses from Members across all of the represented industries and in this paper varying views are represented from some L1 Members, Charity Members, Broadcast Members, L2 Members and Industry Support Members.

Some of aimm's larger Members may input their response directly to the PSA through their regulatory staff or regulatory representatives. Wherever possible, we ensure that views of members made through independent responses are in synergy with aimm's collective views.

As our response is guided and supported by Members input, some views may be expressed that are not necessarily those of the aimm Executive or aimm's Board of Directors

## Response to PSA questions

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.

Different categories of Members had varying views on the data sets listed in Annex A. Whilst not an exhaustive list, most Members spoken to felt that the data listed was probably more comprehensive than that which they retained, and that no one entity would generally collect /retain everything on that list. It was felt more that the data as a whole would be collected across the service chain, so might have to be requested from other entities if the PSA required it. Some Members felt that the list represents a heftier requirement on this industry than seen in others. One Member suggested that all data sets listed underneath 'Transaction logs' in Annex A may not be accessible for merchants, difficult for them to obtain. And asked for clarity on whether merchants will be given any kind of flexibility when it comes to obtaining this third-party data. One Member queried the collection of IP addresses and asked what useful information -as these are no longer static - could be gleaned from storing something which could refer to a group of people.

One group of Members stated that the Relevant Data could be split down into sub-categories in order that more appropriate retention limits (and in some cases no retention requirement at all) be applied in a manner that was more reasonable and easier to manage.

Many Members identified various individual items that they felt should be clarified further in any final list and it was generally felt that the list could benefit from each item being further explained and justified to ensure their meaning was beyond doubt. Again this is due to the differing nature of each party in the chain and the data they collect/retain. Some Members stated that they simply would not need to collect or store some of the items listed (especially for less complex products/services).

Additionally, some Members noted that the proposed Guidance covers retention of broader sets of information, not just personal data and goes on to say that it covers:

“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”)

These Members felt that this phrasing, particularly “any other information that may be of evidential value” and “any related or other information that may be relevant” is too vague to be of use, and subjective to the point where the Member may fall foul of this regulation due to their view of relevance.

A group of Members stated that trend analysis and other similar data manipulation can be a manual activity which will be additional to existing work. It may be that it can be done retrospectively if required for a complaint but is unmanageable if required on an ongoing basis for each product/service. These Members feel that the level of complaints that they receive does not warrant collecting this amount of data going forwards.

**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?**

Members note that the PSA proposes that all Relevant Data should be retained by all those involved in the provision of phone-paid services for two years as a minimum from the point at which they are collected. Some Members agreed that this was reasonable. A group of Members feel that this may be in conflict with their contractual arrangements and it was noted that, in some cases contractual arrangements are more onerous than the PSA requirements.

Another group of Members felt that two years was in fact too long, and that one year would be sufficient to balance regulatory requirements with the GDPR obligation to minimise data. One Member suggested that where a complaint is turned into an investigation, this will most likely be an investigation of a service rather than one individual case, and in those circumstances evidence will continue to be generated, with little reliance on older evidence over a year old.

Some Members requested confirmation from the PSA that - should a data subject ask to be forgotten - the PSA requirement to retain their data will take precedence.

**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?**

Members were divided here, with some Members suggesting (whilst others disagreed) that there is no evidence to support a requirement for three years retention in this area, and questioning why our industry is being made a special case in this respect. One Member questioned the storing of this data at all, as they do not believe it relates to consumer rights. However, another group of Members suggested that they already retain DDRAC data until the end of the contract (which in many instances may be longer than three years), and would like to continue to do this whilst implementing this minimum retention period in case of shorter contractual agreements.

Some Members would like to see further explanation around the wording in this area. As previously mentioned, under the 'Rationale for New Expectations' section, the phrasing:

“ 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”)” causes concern due to its subjectivity and needs clarification.

creating the conditions for growth in micropayments

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.

Most Members did not have an issue with data being retained during an investigation however concerns were raised that there appears to be no limit on the length of time that an investigation can take. They state that, should an investigation begin towards the end of the original retention period, this could realistically mean a prolonged period of time of retention, becoming onerous on the Member concerned and an unnecessary infringement of a consumer's data protection rights. Some Members would expect the PSA to monitor the length of investigations from a summary view (to note the general length of time an investigation takes, therefore enabling identification of those that are exceeding acceptable timescales) and individually to ensure that investigations are making sufficient progress. Investigations that become stagnant for a prolonged period (to be agreed) should be closed down to allow retention requirements to cease.

Some Members questioned why they would need to retain evidence pertaining to an investigation once it had been submitted to the PSA (as such duplicating the data rather than minimising it).

Members generally would expect that the PSA to be explicit when an enquiry becomes an investigation so that there is no chance of confusion in this area, and that once evidence had been submitted and receipted, they should be free to delete it after the two/three year period.

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?

A group of Members questioned whether the justification around keeping some of the requested data (i.e. being required by regulation) is enough to balance GDPR data minimisation requirements. Some Members questioned what would happen should there be a conflict of interest (for example should a Data Subject wish to deny consent, or exercise their right to be forgotten and deleted, during an investigation). Generally Members feel that the regulatory obligations trump the 'forget me' request, but would like the PSA to provide clearer information in this area, however some Members suggested that a consumers rights to exercise control over their own data should be protected, and that these proposals are in opposition to that right.

A group of Members requested clarity over the retention of CLI/MSISDN/IMEI/IMSI or IP address data (and any other associated data) that gets transferred to a different person (i.e. following the sale of a mobile phone). Should this data still be retained if it no longer correlates to the original owner?

One Member suggested that GDPR advice which they had received before May 2018, had stated that data should be retained from the period that the data subject ceases to use the service, rather than the date of collection of the data (in this document) - leaving them unsure about how to proceed.

One Member questioned whether the data requirements were grouped appropriately and suggested that it could work as follows:

- (1) Evidence of consent to charge
- (2) Evidence of supply of required system messages
- (3) Service content
- (4) Merchant to consumer communications about the service
- (5) Evidence about the service provider/s

This Member suggests that there are elements of what could be classed as the 'service content' group (categories (a), (b) and (j) on page 8 of the consultation document) that may not have much value but could be the most sensitive (i.e. dating service content). Their view is that there are some services where service content is in no way useful for resolving the investigation and as such should be minimised.

Members noted the recent GDPR statement released by the PSA on 26<sup>th</sup> March. In this release the PSA answer queries on whether consumer consent will be required for providers to pass consumer's personal data to the PSA in response to a preliminary enquiry. It is stated that *"the legitimate interests of consumers will be served by the processing taking place as the processing would form part of a timely regulatory process, which seeks to address matters raised in consumer complaints to PSA. As stated above consumers are likely to expect processing of their personal data to enable such matters to be addressed. In circumstances where another person has made a complaint on behalf of the user of the service or the bill payer there remains a clear benefit to them in a regulatory process that looks to safeguard their interests through gaining an understanding of consumers' experiences of a particular service and deciding how best to address any issues that are identified from such experiences"*.

This appears to be the only reference to a situation where someone is making an enquiry on behalf of someone else, and some Members are keen to get more clarity here. This paragraph seems to suggest that a consumer calling the PSA and providing a phone number can get information on the services that have been accessed by that MSISDN, including dates and times without identifying themselves. Members are concerned that this might be a breach of privacy which should be addressed to prevent potentially sensitive data being given out to someone who is not the owner of the device. Members suggest some form of verification, such as a PIN being sent to the MSISDN and confirmed back, to ensure that potentially sensitive data being accessed by someone who is not the device owner.

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?

Other than the information already provided in this response, generally Members were keen that any proposals should not be retrospectively applied but implemented at an agreed time to allow industry to deliver effectively. Members requested clarity on whether guidance would also only apply to any data collected from the implementation date - not before.

A group of Members stated that the costs within the consultation document are underestimated and that these requirements will require substantial funding. The costs of storage is not just limited to hardware but must cover additional administration and supervision costs, as well as further hardware

required to support back-ups. Existing systems will also need amending to collect the additional data required, incurring significant cost. These Members ask that the PSA consider the impact of these costs in their balanced approach to regulation.

One Member categorically did not agree with the proposals in this consultation and wanted to instead to see suggestions which would reduce the amount of time that data is held. They stated that new regulations that would improve efficiency of investigations and act to further consumer rights would have been most welcome.

Our response has been made constructively, compiled from member input and with the intent of achieving an effective, fair, economical and proportional regulatory regime for phone paid services in the UK. If any clarification to our response is required or if we can be of any further assistance please contact me personally at [joanna@aimm.co](mailto:joanna@aimm.co)

Regards,

Joanna Cox