Consultation response form

Consultation on revised guidance on Consent to Charge

Please complete this form in full and return by email to consultations@psauthority.org.uk or by post to Mark Collins, Phone-paid Services Authority, 40 Bank Street, London, E14 5NR.

Full name	[redacted]
Contact phone number	[redacted]
Representing	Organisation
Organisation name	Donr Ltd
Email address	[redacted]

If you wish to send your response with your company logo, please paste it here:

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.

Personal data, such as your name and contact details, that you give/have given to the PSA is used, 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 subscriptions review and publish the 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.

Confidentiality

We ask for your contact details along with your response so that we can engage with you on this consultation. For further information about how the PSA handles your personal information and your corresponding rights, please see our privacy policy.

Your details: We will keep your contact number and email address confidential. Is there anything else you want to keep confidential?	Delete as appropriate: Nothing
Your response: Please indicate how much of your response you want to keep confidential.	Delete as appropriate: None
For confidential responses, can the PSA refer to the contents of your response in any statement or other publication? Your identity will remain confidential.	Yes

Your response

Please enter your response to each of the consultation questions in the appropriate box below.

Consultation questions	**Your response**
Q1. Do you agree with our definition of informed consent at paragraph 1.4? If not, why not?	Confidential? No We are happy with the bulleted definitions of consent; however, the following statement needs further clarity: “tamper-proof, independently and easily auditable record” For high risk services, it has generally been accepted that practically speaking, this condition is fulfilled by storing a copy of the HTML, CSS, JavaScript and Image files on a third-party platform such as Amazon S3, with version control enabled. This provides an independent record of the assets shown at the point of purchase with a version log to provide a history of changes. Whilst this is acceptable for “high risk” classed services, it is somewhat impractical for low risk services. As a compromise, a templated approach would be suitable. This allows a single template to be stored, with all users seeing the same version whilst simplifying the logging processes.

Q2. Do you agree with the changes to Section Two of the Guidance at paragraphs 2.9 to 2.13? If not, why not?	Confidential? No 2.9 – We do not agree that the text highlighted in red should be included: Instructions on the website should make clear that the consumer has to enter the PIN which they received within the MT message into a second field, which should be located beneath the first field where the consumer entered their number. The user experience for a second field should not be prescribed in this way and from our experience this form of flow is impractical on smaller screen devices. A better experience is to break the stages into steps, with a MSISDN entry step then a PIN step. This allows spacing, explanations and navigation options to be appropriately laid out. 2.10 Historically, the service name and pricing information is not included in the MT message to prevent this method of consent being used for unsolicited marketing. Within the proposed approach, there is nothing to prevent a rogue merchant entering MSISDNs and triggering the MT message to consumers. The consumer is then presented with a message that can be constructed in such a way they can be misled into replying and circumventing the intent of this safeguard. Traditionally, this was addressed by omitting any service information, including appropriate pricing information and a statement about deleting or ignoring the message if received in error. 2.11 It is not our understanding that all mobile operators retain this data for the 24-month retention period. Additionally, whilst the data shows the consumer is using data, it is not our understanding that more useful information is available such as the website URL they are visiting. 2.12 No comment 2.13 This appears to handle subscription flows, but does not reference single donation/ purchases, which would not be required to meet the recurring donations/ subscription special conditions.

Q3. Do you agree with the proposed Technical Expectations? If not, why not?	Confidential? No Within the technical objectives, it is desired that JavaScript files are hosted by the L1 provider to enable auditable records. To enable them to do this, a facility is required to allow the JavaScript file and code to be uploaded by a Level 2 provider. This upload process essentially requires an L1 to accept JavaScript files, which creates an inherent security risk as the files could (but highly unlikely) contain malicious code. The result of this is the uploading process would not meet the CVSS 4+ standard required. The PSA should consider which risk is acceptable, as it is not possible to satisfy the conflicting requirements: Either: ▪ The L1 to host and log JavaScript files and capture the entire purchasing experience; or ▪ To meet the CVSS 4+ requirement and not permit the L1 to accept any JavaScript uploads It is our understanding that we have extensive experience in this area as we are the only provider to not permit Level 2 providers to host any payment pages themselves. Once this standard is adopted across all L1s, we believe this issue will become more prevalent.
Q4. Do you agree with the proposed Staffing and Training Expectations? If not, why not?	Confidential? No 3.6 We strongly disagree that staff roles and experience should be prescribed in this way. By way of example, a better approach is to engage independent security firms who are exposed to front line threats across a multitude of websites and organisations. They will be aware of threats significantly quicker than in-house personnel and will have access to a wider range of talent to cover different specialities. Regular, routine monitoring by an independent security firm would be able to feed into a development team that is able to focus on implementing recommendations, rather than wasting time trying to

	discover information about threats that may not be in the public domain. 3.7 Whilst the spirit of this proposal seems well intended, we question its place in a guidance document. As has been seen with the recent adjudication against VEOO, a bad actor ignores guidance as it is non-binding on the 14th code. We would suggest the intent of this clause is situated in the 15th code (when released), with appropriate considerations given to how the PSA can review and enforce the proposed processes.
Q5. Do you agree with the proposed Risk Control and Incident Response expectations? If not, why not?	Confidential? No Whilst they appear practical on paper, timescales should be considered as some of the changes are significant and affect core platform functionality. It would also be significantly beneficial for changes to be planned with the MNOs and other PSA projects to allow focus and opportunity to implement. Within the cost proposals, MNO imposed costs should also be considered. We also feel the suggested salary ranges are excessive, perhaps London biased and therefore disproportionate. In the context of costs, the near doubling of MNO costs in the last 24 months, along with increased cost to fund PSA requirements will necessitate a shift in budgets. This raises the question; How should L1s be effective gatekeepers for services when there is increasing demands to shift their income to MNO 'required' services or ring fence to areas at over-inflated rates? As was evidenced by the VEOO tribunal, once front-line training, support and knowledge is de-funded, standards deteriorate and consumer harm is created. Whilst it is acceptable to pass this cost on to merchants, PRS services are already significantly higher than card payment services and in the case of Donr, this would reduce the income our charity clients receive from their donations.

If you have any supporting imagery for your responses, you can paste them in your responses in the table above or here:

Submit your response

To send your responses to the PSA please email this completed form to consultations@psauthority.org.uk or by post to Mark Collins, Phone-paid Services Authority, 40 Bank Street, London, E14 5NR.