# ISSUE-235: Auditability requirement in Reasonable Security section

## Summary

This question addresses ISSUE-235. For more information please refer to the wiki page. The results of this CfO are documented here.

In conclusion, ISSUE 235 is closed. We determined that Option 1 received weaker substantiated objections and is therefore determined as the consensus of the group.

## Detailed Argumentation

### The Options

#### Text Proposed by Option (1): Remove auditability requirement from security section

***Remove*** *the text below from the Reasonable Security section.*

Third parties SHOULD ensure that the access and use of data retained for permitted uses is auditable.

#### Text Proposed by Option (2): Add explanatory text for "auditable"

*Retain existing text and add the following paragraph to the Reasonable Security section.*

For the purposes of this recommendation, **auditable** is understood as having sufficient records of access and use of data retained such that an independent auditor would have a reasonable level of confidence that the data retained is exclusively used for the permitted uses or that breaches of this can be detected ex-post. For example, an auditor might use a similar level of confidence to that required for the organization's financial records.

### Received Input

We received inputs from 4 individuals/organisations.

#### Objections against Option 1: Remove auditability

We received multiple objections against option 1. The primary objection (by Walter van Holst and Mike O'Neill) was that if the auditability argument is removed, companies no longer need to record accesses and as a consequence, no evidence of potential data misuse would be available. David Singer objected to not placing auditability requirements on companies, but noted that that would be required whether the text was present or not.

### Assessment of Objections against Option 1

Being able to validate correct behavior and detect misuse of data is a worthwhile consideration. However, a vague data retention mandate will do little to accomplish this goal. Private citizens will be unlikely to access this data in order to review it. Regulators already have existing legal requirements to obtain information from data controlllers and processors, and to require them to maintain that data in order to document processing. The proposed language did not offer sufficient clarity to implementers as to what information would need to be preserved.

### Objections against Option 2: New Non-normative Text

We received multiple substantiated objections against option 2. The objections were mainly focused at the explicit auditability requirement (and less against the extra text).

One objection to this proposal was that existing approaches (including but not limited to audits) should be sufficient to validate correct behavior (Shane Wiley). A second argument made (by Roy Fielding) was that strict auditability may have undesired privacy implications. Both argued that this language would be difficult to implement.

### Assessment of the Objections against Option 2

We determine that the objections against Option 2 were more strongly substantiated. It is unclear from the proposed text was precisely companies would need to do in order to meet this requirement. Given existing legal obligations, it is not clear that the proposed text would offer consumers and regulators greater accountability from companies.

## Results

Overall, we rated the objections against Option 2 as more substantive and followed the arguments that existing best practices should be sufficient to ensure compliance in practice.

In conclusion, ISSUE 235 is closed. We determined that Option 1 received weaker substantiated objections and is therefore determined as the consensus of the group.