22 August 2019

CONSULTATION DRAFT - CONSENT MANAGEMENT AND REVOCATION
NAB FEEDBACK

- Great work on creating guidelines that are easy to consume, and thoroughly documented. It's a great step towards creating consistency for consumers.
- To ensure consistency for consumers, NAB requires that Holders and Recipients **show the same information in a consent arrangement and show that information consistently.** This is even more critical for joint account and business scenarios in which a secondary account holder will have the added context of the sharing arrangement to make an informed decision.
- The **Data Language Standards must be extended** to include terms for all consent stages and actions for managing the consent, not just the clusters. This is something that should be enforceable to drive consistency across all participants for consumers.
- The inconsistency in standards don't allow DHs to have visibility of the '**consent to de-identify** data during data sharing'.
  It's important to share the same consent details in both DR and DH to **ensure a consistent experience for the consumer.**

Questions that we would like answered

- What is the intention going forward with **granular consent? We require clarity and alignment from CX guidelines and technical standards** to move forward with build. Given this remains unresolved, then it will need to be a requirement for later phases.
- **Downloading the records of consent data collected** - This is outlined as a rule (CDR rules, 9.5); we haven't seen any discussion around this and remains an outstanding issue. It's unclear how we can meet our compliance obligation in relation to this rule. We would like to see when this will be addressed.

Item, Page, or Guideline	Feedback
Page 4, Use case view & Data sharing arrangement view	**Use case view is not currently possible for Data holders;** within the current standards we have no visibility on use case. Data sharing arrangement view: Again, the descriptions under "Why we need it" cannot be populated with the

	current technical standards for Data Holders – this is beneficial for consumers to identify consents and differentiate between use cases that might share similar scopes
Page 6, Guideline 1.5 - **Search**	Consider outlining that filtering can be by Data type, Organisation, product, timeframe.
Guideline 4.1 and guideline 4.4 **Arrangement**	Holders and recipients must be consistent when showing the same information to consumers. This can be done by using consistent labelling for groups of information. Examples: Scopes should be the same (data and purposes), ‘duration of data sharing’ vs ‘data sharing details’, De-identification of data must be played back in DRs an DHs arrangement. This is even more critical for joint and secondary and account considerations
Guideline 4.1	What happened to the data should be surfaced once sharing has expired. This should be available to DRs and DHs
Page 8, De-identification within duration	From a consumers point of view, this must be a separate consent. What’s happening with this? I understand this as DRs capturing consent to help improve their product offering by learning from the data that has been shared. If this is the case it should be phrased in that way. ‘We have your consent to de-identify your data outlined above so we can analyse it and to see how we can improve our service.’ If this was something that could be optionally consented to in the first authorisation, consumers

	should also have the ability to revoke granularly as well. There should be guidelines created **Additionally, this is a consent a joint or secondary account holder will not have visibility on.**
Guideline 4.3 Updates to the consumer dashboard	This is unclear if it is referring to editing the consent during its lifecycle or adding the consent to the dashboard.
Guideline 4.4, Arrangement data collection (data holder)	'How often data is shared' is in the imagery, **but that is not possible for data holders.**
Guideline 4.4, Arrangement When the consumer gave authorisation (data holder)	Also consider who gave authorisation, in joint scenarios.
Guideline 4.10 Withdraw consent	Consider communicating that consent withdrawal only requires one party, not all.
Language	Are there any language guidelines on the wording around where a connection is active? I.e. Wireframes use phrases like: ▪ Sharing ▪ Currently sharing ▪ Consent expired What should the wording be for when an DRs accreditation status has been revoked? What should the wording be for when an DRs accreditation status has been suspended? **Consistent language statuses across participants will greatly benefit consumers**
Page 4	"Stop sharing all data" action on "Product specific" and "Use case specific" pages, appears to indicate that this

	would support **bulk revocation** of multiple data sharing arrangements. Is this intended?
Page 8	Display of accounts shared with a Data Recipient on the DR dashboard could be out of date if consumers can change the accounts to be part of data sharing. The CDS API/InfoSec technical standards do not support any notification from DH to DR when a consumer alters (via the DH dashboard) which accounts they want to share. Similarly, if the consumer stops being an account holder of the previously shared account, then data sharing from that point will cease. The CDS API/InfoSec technical standards do not support any notification from DH to DR to support such scenario.
Guideline 5.1 Revocation	**Revocation can highlight two scenarios:** Revoking and deleting data. Revoking access and keeping shared data. The option should be available to consumers. ME Bank presented a good example of this in their presentation last week.
Joint revocation	From a DH dashboard perspective, for joint account holder scenarios, what is the expectation when the joint account holder who did not set up the initial data sharing performs the revocation. Would this revoke the entire data sharing transaction, including sharing of single owned accounts? Or is it only removing the joint account from the data sharing connection, which will continue to remain active for the non-joint accounts? If the latter, how will DRs be advised of this? The CDS API/InfoSec technical standards do not support this kind of event / action notification.
Account level granularity	We should allow consumers to **add or remove accounts from an arrangement** over its lifecycle. It doesn't necessarily need UX, but it can be outlined as a consideration for Data Holders.