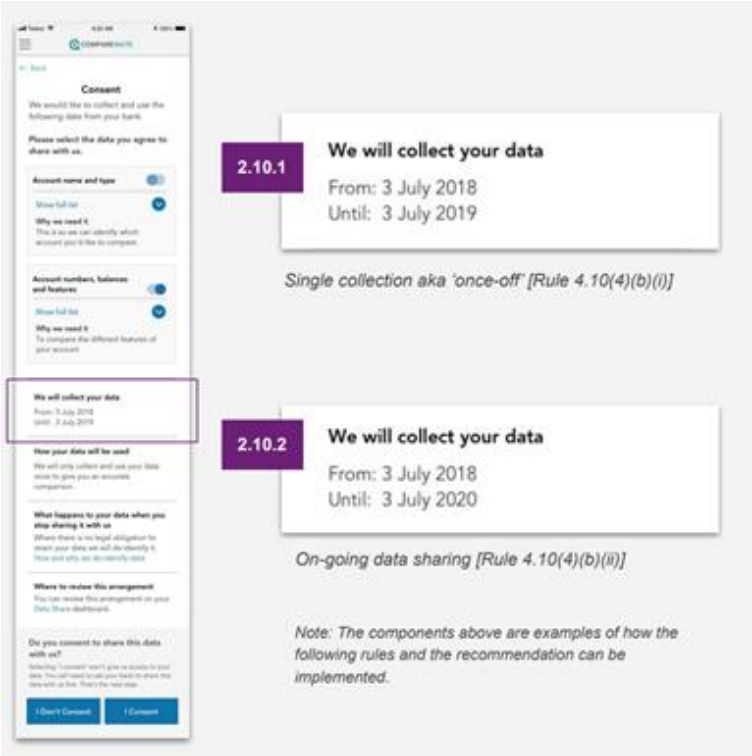
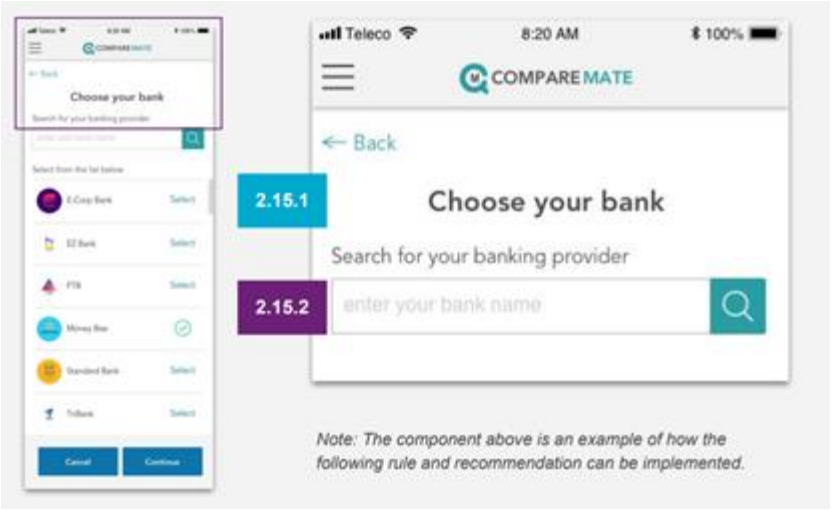
CBA Feedback: Data61 CX Guidelines version 0.9.5

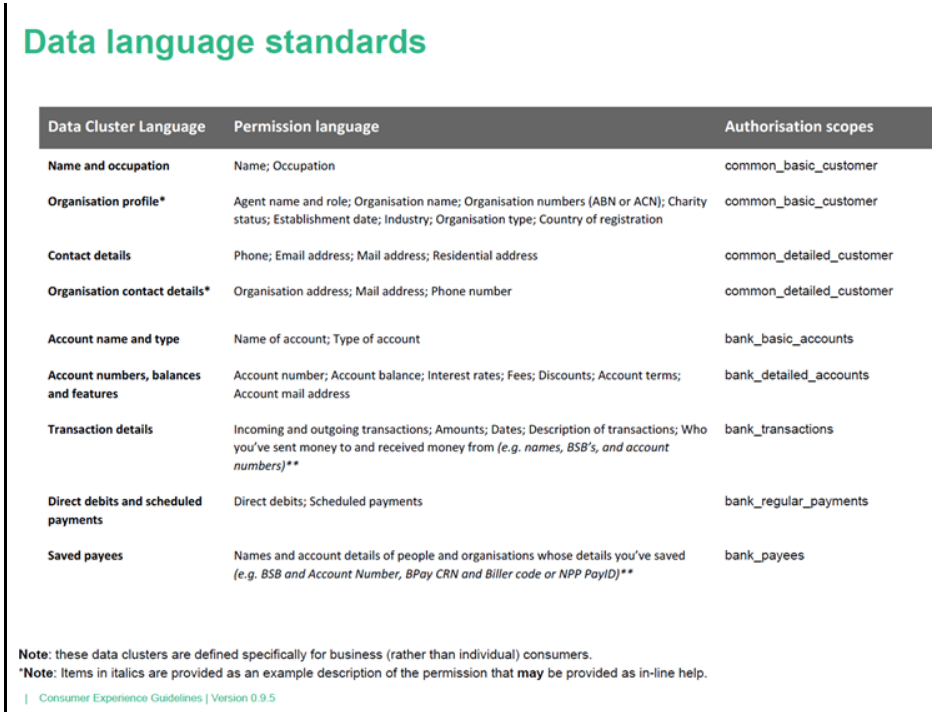
CX Guidelines Pg ref.	Document Section	Feedback & Clarifications sought
39, 40 38	**2.4.1 Mandatory** The data recipient **must not** include documents or references to other documents that reduce comprehension. Any links to information that increase comprehension **should not** take the consumer to an external page. *CDR Rule 4.10(2)(c), 4.16(2)(c)* **2.4.2 Recommended** The data recipient **should** provide information, where applicable, about measures taken in case of security breaches. *CX Research 14* **2.3.1 Recommended** The data recipient **should** present any trust mark required by the ACCC to provide consistency and facilitate consumer trust. The data recipient **should** provide a way for consumers to verify their accreditation via the ACCC. *CX Research 13, 23*	2.4.1: Can Data61 confirm the definition of 'External page' – does this mean a site not owned by the Data Recipient (eg. the ACCC 'one pager' referenced in testing reports)? How does this sit with 2.3.1, recommending customers should be given a way to '*verify their accreditation via the ACCC*'? This couldn't be done without providing external links. In addition, the CDR policy would typically be accessed via a link in the consent flow to another page or PDF for the customer to view or download.

46	**Mandatory** The data recipient **must** allow the consumer to actively select or actively specify the types of data and the uses they consent to. If data is being requested for multiple uses, the consumer **must** be able to specify which uses they consent to. The data recipient **must not** rely on, for example, pre-selected options to indicate the data that the consent relates to. The data recipient **must not** infer consent or rely on an implied consent. Achieving the above **may** involve using various consent capture design patterns that allow consumers to opt-in such as checkboxes, toggles, and binary yes/no choices. *CDR Rules 4.10(3), 4.16(3) | CX Research 2, 3, 4, 5, 6*	We agree that the principle of customer control over the data being shared is an important one, however we believe the issue of data minimisation is better achieved through scope granularity rather than customer opt-in. Given data recipients should adhere to the data minimisation principle, they should only be requesting data required for their use-case. If all data clusters are required by the DR in order to provide the feature/use-case to the customer, if the customer does not select all clusters, they may be unable to access the feature/use-case. We are concerned with the poor customer experience of asking a customer to assess and opt-in to clusters one-by-one, only to be unable to continue if they do not give consent to specific clusters. For example, a credit card application may request access to bank_basic_accounts and bank_transactions, since basic account is required to get transactions. If the customer did not opt-in to basic accounts, but did opt-in to transactions, there is no way to provide the use-case to the customer. We recommend this mandatory requirement is changed to a recommendation, or at a minimum that data clusters are opt-out rather than opt-in.

51	 **2.10.1** **2.10.2** **Mandatory** The data recipient **must** state the sharing duration, including how far back in time data will be collected. The data recipient **must** state if they are requesting consent for a single collection (aka once-off) or for collection over a period of time of not more than 12 months (aka on-going). The data recipient **should** allow the consumer to specify the sharing duration, including how far back in time data will be accessed. The data recipient **should** present the range of collection and use in a way that is easy to understand and appropriate for the use case. *CDR Rule 4.10(4)(b), (c) and (d), 4.16(6)(b), 4.12(1)(c), 4.18 | CX Research 4, 5, 6*	1) The UX in 2.10.2 is inaccurate in that it combines 'collection' access dates with the historical data range being collected. That is, collection would be from today (3 July 2019) to 3 July 2020. The portion of the data from 3 July 2018 to 3 July 2019 (today) is historical data, not collection access. This would better be represented as: *We will be able to collect your data:* *From: today* *Until: 3 July 2020* *We'll be able to access your <data type> data ranging from 3 July 2018 until 3 July 2020.* Historical data is only relevant for some data clusters (eg transactions) so to apply the blanket dates above in a scenario where you have multiple data clusters (eg Payees and transactions) wouldn't make sense. If we are trying to give total transparency to customers, we need to be clear about the collection period vs the historical data range being collected. 2) Clarification is sought regarding '12 month' consent period. The UX shows '3 July 2018 to 3 July 2019'. Our legal interpretation of 12 months would cover '3 July to 2 July'.

58	 **2.15.1 Recommended** Data recipients **may** choose to present data holder selection screens before or after the data request occurs. **2.15.2 Mandatory** Data recipients **must** make data holder list searchable. *Nielsen and Molich's 10 User Interface Design Heuristics: Flexibility and efficiency of use*	2.15.2: we agree that search is best practise design, however we suggest this requirement is only mandatory where the list of data holders exceeds what can be viewed on one page – if all data holder options are visible without scrolling, a search bar is redundant.

74	**4.4.1** **4.4.3** **Mandatory** The data holder **must** state the sharing duration to the consumer, including how far back in time data will be accessed. The data holder **should** present the range of collection and use in a way that is easy to understand. *4.22(2)(b) and (e)* **4.4.2** **4.4.4** **Mandatory** The data holder **must** state whether data will be shared for single or on-going collection. *4.22(2)(d)* **4.4.2** **4.4.4** **Mandatory** The data holder **must** state how often the data will be disclosed over the specific period. *4.22(2)(e)* **4.4.3** **Mandatory** The data holder **must** notify the consumer of the expiry date of their data sharing. *CDR Rule 4.25*	4.4.2, 4.4.4 Currently the data standards do not include a field for frequency of disclosure/access in the request payload. As such there is no way for the DH to know what to display to the customer as depicted in the UX screens. At best, if the request is for 'ongoing' access, a DR could provide a generic statement that won't be specific to the Data recipient's access frequency. For example *"<DR> may access your data up to 4 times a day offline or whenever you log on*". If a DH is required to state how often the data will be disclosed with specificity, a frequency field would need to be added to the request payload from the DR. 4.4.3 The prototype references "We will share your data" and lists a date range. What are these dates based on? In a '**One off'** scenario, there is currently no request duration in the request payload, so we cannot tell the customer how far back the data is being requested. In order to provide this information to the customer, consent duration information would need to be sent in the request to the data holder.

25		1) For scopes where there are basic & detailed options, the 'detailed' is always inclusive of the 'basic' payload as well. This is not reflected in the permission language, meaning that if a DR requests 'Detailed' scope, the customer is not presented with the 'basic' permission language. For example: DR requests common_detailed_customer (individual customers) The permission language would read "*phone, email address, mail address, residential address*" but would not read "*Name, Occupation*" which are parts of the payload as well. We recommend 'detailed' scopes have their permission language updated to include that of the corresponding 'basic' scope. 2) Bank_Basic_accounts includes balances, however this isn't reflected in the permission language. We recommend it is added. 3) Common_basic_customer – how will a data holder know which data cluster/permission language to display (consumer or organisation) during authorisation? There is currently no way for a Data recipient to send this in their request.