EnergyAustralia feedback - CDR consent review # 273

EnergyAustralia would like to provide this written feedback to the consent review, focussing on our views where they were different to the stakeholder views from the workshop which the DSB summarised.

With regard to 1. Pre-selection of data in the consent flow, and 2. Data language standards - relaxing the permission language as to how data is described, more consultation is required on the details of these proposals for stakeholders to provide meaningful feedback.

We do not support the following proposals as described in the paper:

- 3. Withdrawal of consent information (where the DSB noted low opposition),
- 4. Authentication information (where the DSB noted low opposition),
- 5. Supporting parties,
- 6. 90 Day notifications,
- 8. Removal of Dashboards for one off consents, and
- 10. Separation of consents (bundling) (where the DSB noted low opposition);

and consider that removing or bundling this information will remove salient details that are pivotal to the customer's understanding of consent. In particular:

- **4. Authentication information**, which states the customer does not need to provide their password, has heightened importance in the wake of the Optus and Medibank data hacking, and low customer confidence around privacy and data security. This information educates the customer so they don't provide password information to ADRs which might misuse it. It is therefore an important preventative measure to safeguard against customer harm, and protect the reputation of the CDR.

- **5. Supporting parties** is key to providing information to the customer when they are engaged. We are concerned that if this information is not presented in the consent flow, the customer is unlikely to ever seek out information on who the supporting parties are and what capacities they act in. i.e. this would require the customer to seek out the ADR's CDR policy which is unlikely to occur even if hyperlinked in the consent flow.

  Supporting parties should be completely presented as it is key to the consent, it shows who will receive the customer's CDR data, other than the ADR that the customer is directly dealing with. Listing who the additional supporting parties are is also important as it shows what the ADR is not doing itself i.e. that they ADR is relying on other third parties to provide the ADR service/product which would factor into whether the customer is confident in the ADR's business. Information about what the different Supporting parties are e.g. outsourced service provider and what that means should also be provided.

- **6. Bundling of the 90-day notifications** requires more consultation, especially on how they can be bundled. The scenario where a customer receives notifications on five consecutive days appears to be excessive, and it is not clear how realistic a scenario this is. i.e. how often would a customer be returning to provide a consent 5 days in a row? The question then becomes what other 90-day notifications will be bundled. The separation of these notifications is important as it allows the customer to pinpoint which consent is reaching a 90-day duration. Bundling them together may make it difficult to clearly draw this distinction and revoke individual consents. We also seek more evidence of customer fatigue and a compelling case for change.

- **8. Removal of dashboards for one-off consents** is a problematic proposal. We do not see that there is a solid reason to treat one-off consents as different to an ongoing consent. Importantly, the dashboard allows a customer to withdraw their consent. A customer may change their mind immediately after providing their consent to the ADR

and wish to withdraw it before the ADR collects their CDR data. Removing the dashboard would prevent the customer from doing so.

- **10. Separation of consents** could undermine the effectiveness of the CDR consent process. Unbundled consent is key to the consent being specific to purpose and essential for the customer to make an informed decision. Unbundled consent also means the customer can consent to one part but not the other, which is important to allow consent to be voluntary and express.

    - Bundling collection and use consents, but not disclosure consents might be worth exploring in further consultation. Collection and use consents might be intuitive to bundle because a customer will likely assume that after an ADR collects CDR data, they will use it.

      However, disclosure consents can be an unrelated concept. They should be kept separate given it relates to further disclosures by the ADR to other businesses supporting the ADR, or critically disclosures to other ADRs and non-accredited businesses e.g. Trusted Advisors and insight disclosures. Transparency and a clear separation of consents relating to these further data disclosures is highly important. This is because these disclosures might result in disclosures to non-accredited parties, outside the CDR regime. Data leaving the CDR regime will not be subject to the same level of regulation. For example, the data security protections that apply to ADRs for CDR data do not apply to businesses outside the CDR regime. Privacy Principles might apply to CDR data where it is also Personal Information and there are some data security principles, but there are general in nature and non-specific. These new and important considerations support the disclosure consent being separated from collection and use consents.

    - As observed in the workshop and well-accepted, consents relating to Action Initiation and data disclosure must be separate, given they relate to very different uses by ADRs.

- **11. De-identification consent** is already a complex area in the CDR Rules. We are not opposed to further review, but the focus of the review should be to ensure that the de-identification consent process make consents clearer and more prominent to the customer.

  It is important to note that de-identification consents directly relate to how much data can be retained by the ADR after the data becomes redundant for the original use it was collected for. Any watering down of de-identification consent to make it easier to obtain, effectively allows an ADR to de-identify more CDR data and retain it. We are concerned that customers will make once off decisions about de-identifying their redundant data without fully understanding the full consequences of their decision. i.e. that an ADR can continue to use that de-identified data after the ADR no longer needs it for its original use, for an indefinite period, potentially years. We expect that consumers will become more concerned about data retention as data becomes an increasingly valuable resource to businesses. The CDR de-identification consent process should be reviewed to ensure that it is adequate in line with this growing nervous consumer sentiment around data retention.