INTERNET
SAFETY
//LABS

Introduction to the ISL Safe Software Specification

Version 1.1

Table of Contents

1 Introduction to the ISL Safe Software Specification

Note: We highly recommend reviewing the Me2B 101 Flash Guides (#1-10 which can be found in our Blog on our website) to familiarize yourself with Me2B terminology, principles and ethos.

This document introduces key terms and principles around the ISL Safe Software Specifications. It's intended to be an overview to the specifications, which are detailed and lengthy.

All of the tests in specification are summarized in sections 6-15, which also include a high level mapping of how the ISL Safe Software Specification maps to both California privacy regulation (CCPA and CPRA) and GDPR. The specification also includes this mapping for each and every test. See Appendix A for a mapping of key regulatory terminology across ISL, CPRA, and GDPR.

2 Glossary

2.1 Attribute

One of 10 qualities (so far) determined to be minimal criteria for a Me2B Commitment being deemed safe and respectful.

2.2 Data Flow Analysis

Data Flow Analysis is the act of evaluating the flow of data into and out of the website/app/service. This refers to the independent evaluation, using network analysis and other tools to understand where and with whom data is being shared. Many of the tests in this specification require data flow analysis. Conducting data flow analysis requires a trained expert in data supply auditing.

2.3 Data Subject, Data Controller, Data Processor, Data Processing

We use the standard GDPR definitions for each of these terms. See https://gdpr-info.eu/art-4-gdpr/

2.4 Illustrative Controls

Illustrative Controls refer to unique tests that are run. A control must be satisfied in order to receive a passing score on a test. This document doesn't include every possible test that is included in the Core Requirements and thus, the controls are illustrative only (and not comprehensive).

2.5 User Experience Evaluation

User Experience Evaluation is the act of evaluating the user interface of the website/app/service. Many of the tests in the ISL Safe Software Specification require evaluation of the user interface. Conducting user experience evaluation requires a trained expert in user experience design.

3 Introduction

The ISL Safe Software Specification is a *safety* specification—in contrast to an *interoperability* specification. The ISL Safe Software Specification is a structured list of tests, with clear passing and failing criteria.

The first version of the specification is considered the “minimum viable” definition for being “safe” technology—the most basic, fundamental measurements of safety. To compare it the full spectrum of digital harms (as described in our Digital Harms Dictionary), version 1.1 of the specification covers only a portion of the described harms.

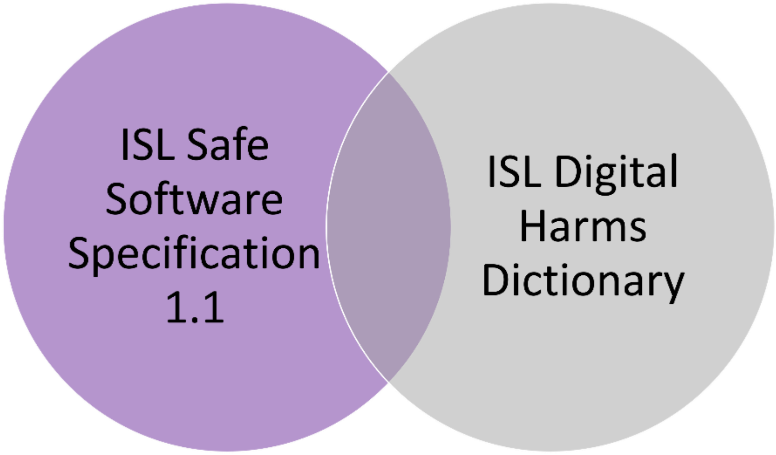
ISL Safe Software Specification 1.1
ISL Digital Harms Dictionary

Figure 1 Relationship Between Spec v1.1 and Digital Harms Dictionary

Over time, subsequent versions of the specification will grow to include all more of the programmatic harms defined in the Harms Dictionary.

4 Specification Architecture

ISL Safe Software Specifications will be produced for each type of connected service and/or device such as:

- Websites
- Mobile Apps
- Wearables
- Medical Implants
- XR Devices/services
- Laptops / PCs
- Tablets
- Automobiles
- Smart Home Devices & Services

Version 1.1 of the specification covers websites and mobile apps.

All the specs would have the same fundamental structure (described below), with some differences unique to the type of service or device. In this way, there is fundamentally one baseline specification that is re-applied and customized as needed for each of the services listed above. The main set of tests will ultimately be stored in a database for easier reusability across services.

The specification is primarily a collection of spreadsheets:

1. Introduction/instructions
2. Data Controller Questionnaire
3. Core Requirements – this is the main body of delineated tests
4. Three files for use by the testers:
    a. Website Raw Data Collection worksheet – for testers to capture information about what data is being collected, shared and with whom,
    b. App Raw Data Collection worksheet – for testers to capture information about what data is being collected, shared and with whom,
    c. Raw Policy Info Collection worksheet – for testers to capture the key promises made in the privacy policy and terms of service, especially as it relates to data processing (collection, use, sharing, etc.)

4.1 ISL Safe Software Specification Organization

Each specification tests each of the Me2B Commitments found in the service's user interface. Each Me2B Commitment represents a distinct value exchange (Me2B Deal), for which the user receives something of value (e.g., information) in exchange for providing something of value, typically in the form of information or online payment. Examples of Me2B Commitments are:

- Pre-Commitment or No-Commitment state (e.g., the state where the individual has opened an app/website/service for the very first time)
- Local Storage Commitment (e.g., Cookie commitment on websites)
- Location Commitment (e.g., providing location information to the service in order to receive location-relevant information)
- Promotional Commitment (e.g., signing up for newsletters)
- Contact Us Commitment(s)
- One-off Transaction (e.g., purchasing something as a guest)
- Loyalty Program
- Account Creation Commitment (I.e. Me2B Marriage, signing up for an account with the service)

Each of these commitments (including pre-commitment state) are tested against the 10 Attributes for Safe and Respectful Me2B Commitments. (See https://me2ba.org/library/recommendation-attributes-of-safe-respectful-me2b-commitments/) Each attribute has one or more unique tests.

Figure 2 below illustrates a simplified view of the testing flow—i.e., how the tests documented in the Core Requirements would be run in practice.

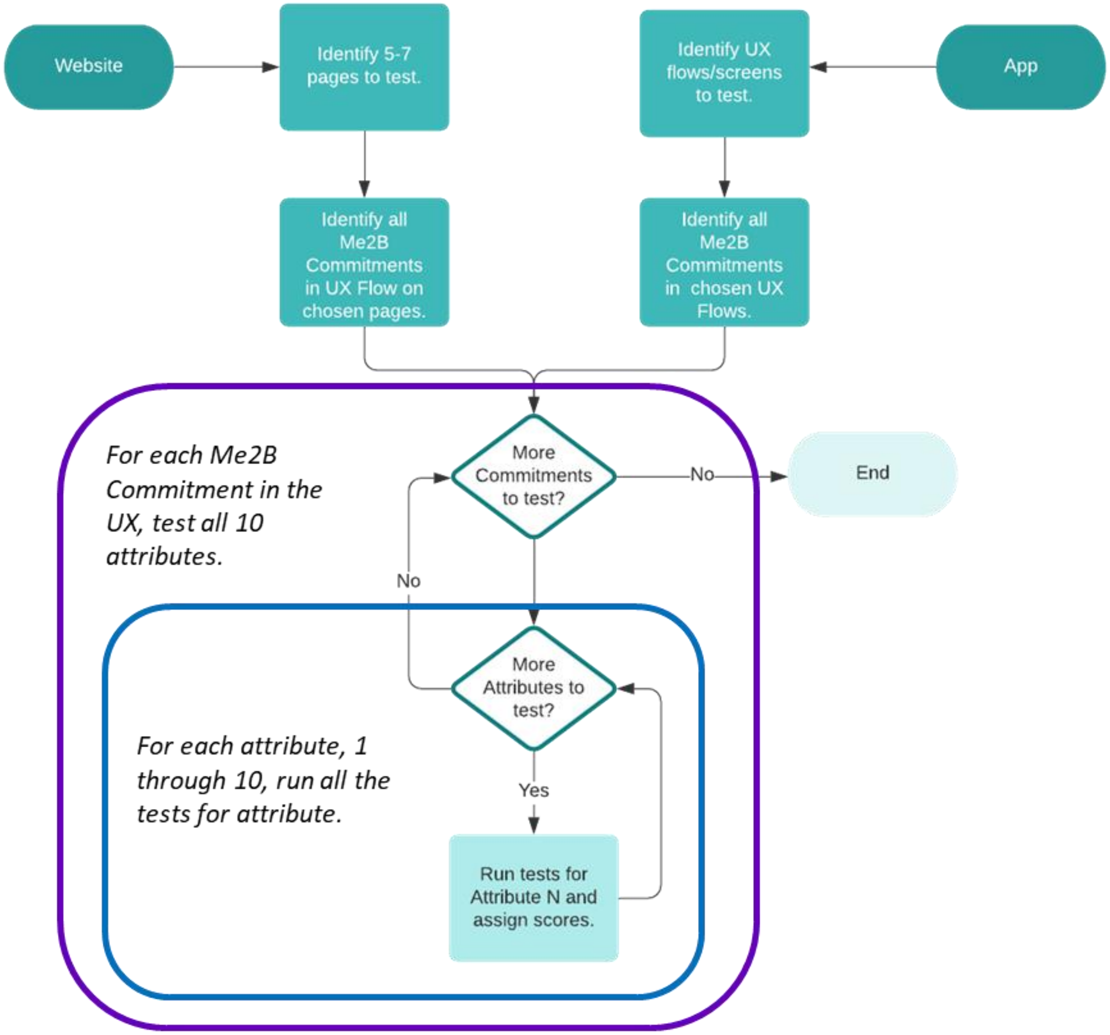
Website
Identify 5-7 pages to test.
Identify UX flows/screens to test.
App
Identify all Me2B Commitments in UX Flow on chosen pages.
Identify all Me2B Commitments in chosen UX Flows.
For each Me2B Commitment in the UX, test all 10 attributes.
More Commitments to test?
No
End
No
More Attributes to test?
For each attribute, 1 through 10, run all the tests for attribute.
Yes
Run tests for Attribute N and assign scores.

Figure 2 Specification Testing Flow

Note that it's impractical to test all the pages in a website—some websites are hundreds of pages in size. So, the first step of the website testing process is to identify the key 5-7 representative pages to test. A similar selection is made before testing a mobile app: determine the key UX flows and screens to be tested. Generally, the intention is to test all the UX flows and web pages that correspond to Me2B Commitments.

Each of those commitments would be tested against the 10 attributes of safe and respectful commitments.

Figure 3 provides more detail about the steps involved in using the specification materials to test a website or app.

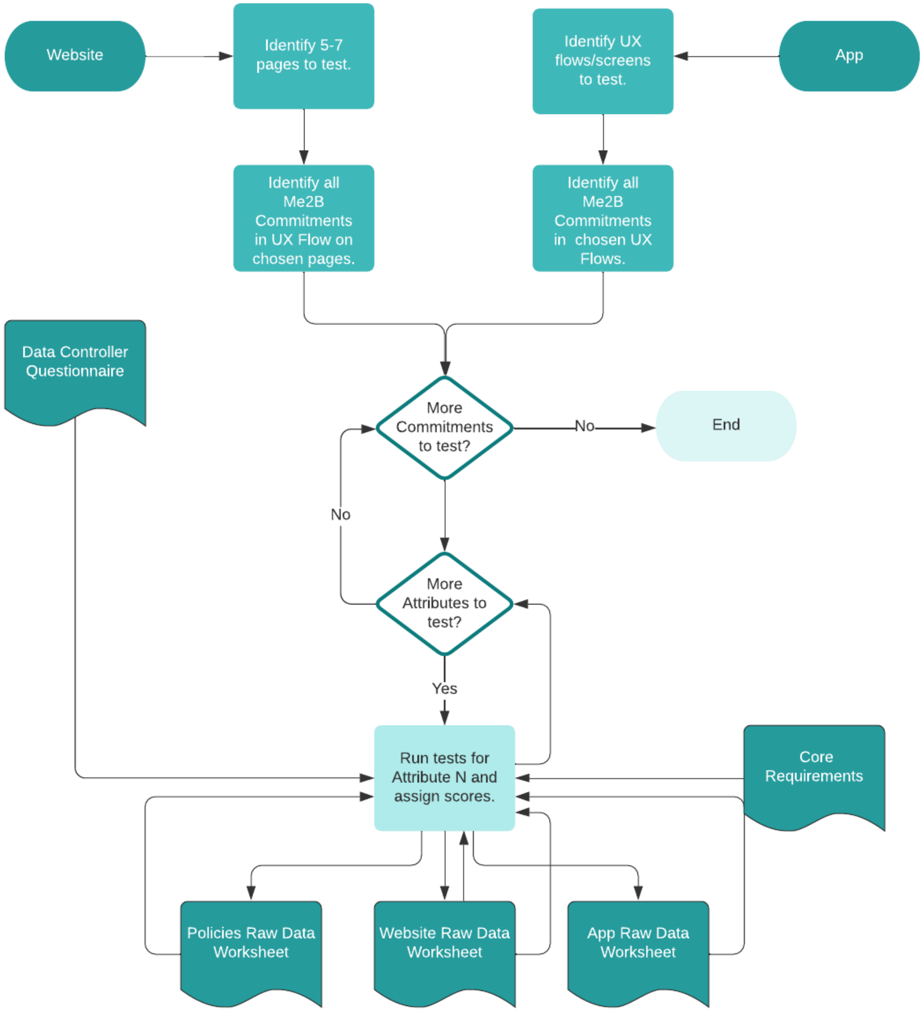
Website
Identify 5-7 pages to test.
Identify UX flows/screens to test.
App
Identify all Me2B Commitments in UX Flow on chosen pages.
Identify all Me2B Commitments in chosen UX Flows.
Data Controller Questionnaire
More Commitments to test?
No
End
No
More Attributes to test?
Yes
Run tests for Attribute N and assign scores.
Core Requirements
Policies Raw Data Worksheet
Website Raw Data Worksheet
App Raw Data Worksheet

Figure 3 Website Testing Process & Spec Use

4.2 Me2B Commitment Context is Key

Why do we structure the testing in this way? Each commitment is a unique point in the overall Me2B Relationship lifecycle, reflecting a certain level of "intensity" of the Me2B Relationship. In particular, a Me2B Commitment is a transaction, with a unique value exchange between the Me and the B. We call this value exchange the “Me2B Deal”, **and for all Me2B Deals, the Me’s *information* is part of the currency of the deal.** It is this truth that creates many risks and harms for Me-s, and thus, why it’s such an important part of the Me2B testing structure; Me2B Commitments can be and often are *unsafe* and *disrespectful*.

Me2B Commitments represent unique points along the arc of the Me2B Relationship Lifecycle. As points on this lifecycle, they reflect not only the particular “behavioral economics” of the moment in time of the commitment, but also the trajectory of the arc—i.e., ascending or descending.

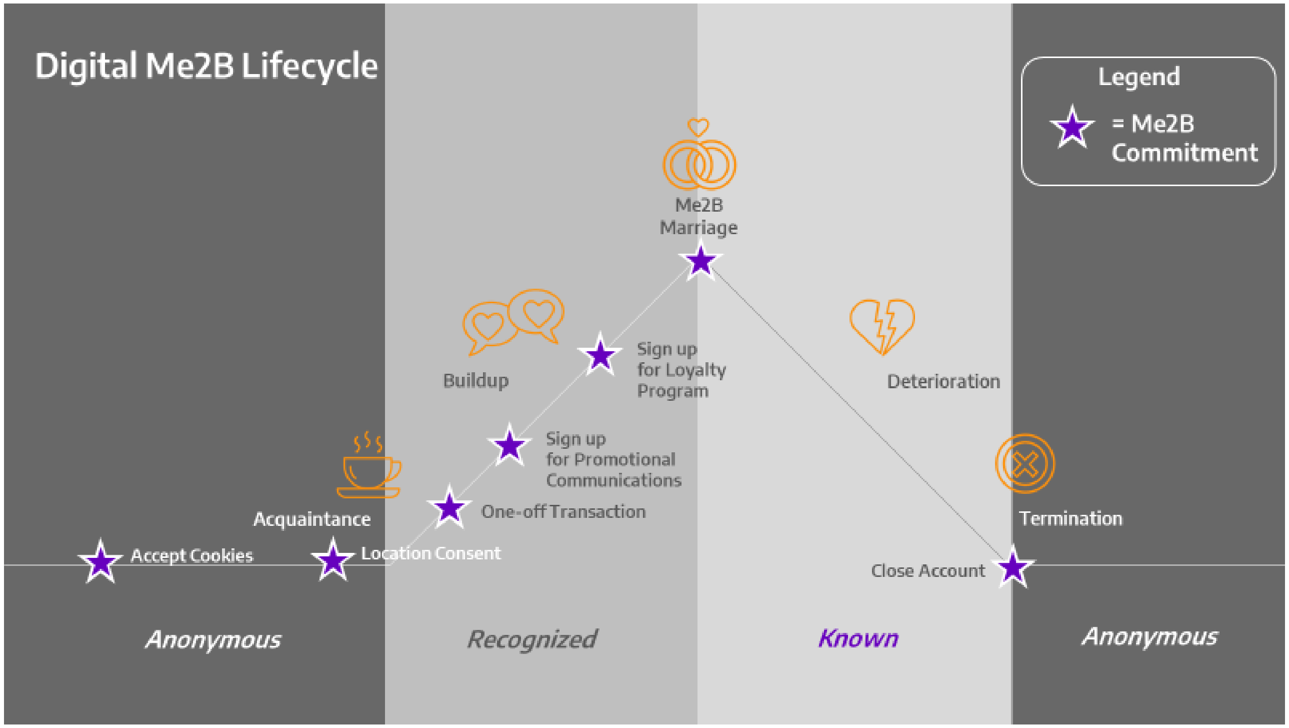

Figure 4: Me2B Lifecycle

A commitment is informed by and reflects three key things:

1. The Me's trust in the B and the B's product,
2. The Me's perceived value and expectations of the benefit to be received and if the cost is equitable, and
3. The vector/direction of the relationship—meaning, if the Me2B relationship is building and deepening, or if it's diminishing. If the Me is sharing yet more information, the relationship is necessarily deepening; if the Me is revoking the sharing of information, the relationship is necessarily diminishing. The only way a relationship vector remains neutral is if the commitment transaction is a virtual "repeat" of a previous transaction commitment.

This relationship lifecycle context mirrors the organic dynamics of our interpersonal relationships—where what we share reflects our trust in the other person, our expectations, history, and perceived value of sharing. We may be so habituated to this kind of behavioral economic calculus that we no longer recognize that we're doing it. In our Me2B relationships in the digital world, the calculus is much more prominent, overt.

Take, for example, the Local Storage (including cookies) commitment. This commitment usually occurs very early on in the Me2B relationship and people's expectations of this particular commitment may be quite low, recognizing this is a kind of "entry gate" commitment. Whereas the so-called "Me2B Marriage" of creating a personal account reflects a much deeper--in fact, the deepest--stage of the relationship, and thus the user's behavioral economics in evaluating the costs/benefits of the deal (i.e., creating an account, being remembered, recognized, and personally responded to) are potentially (and hopefully) more thoughtful, meaningful.

To say it another way, each Me2B Commitment has tolerances that are unique to the level of the commitment and where it is on the Me2B Relationship arc. This "context sensitivity" is central to the ISL Safe Software Specification. **Without this commitment-specific context, it's virtually impossible to derive objective scoring criteria.**

In addition to the tests that map to the commitments listed above, there is also a list of tests that are "commitment-agnostic" and apply unilaterally to every website, app or service being tested. These "commitment-agnostic" tests include high level security tests.

A note on security: The ISL Safe Software specification is, by design, ***not*** a robust security certification. There are already many mature specifications for validating system security and practices. We chose not to duplicate those, but to confirm that some of the key best practices have been adopted.

5 How to Read the Tables in this Document

This introductory document communicates the high-level tests used to assess a commitment against the ten attributes for safe and respectful commitments. Each attribute has a summary table that includes:

- The attribute (high level principle) to be audited,
- The assessment criteria for the attribute, and
- Illustrative controls to measure the attribute; note that these are “illustrative” in that the list may not cover every test in every commitment.

6 ATTRIBUTE 1: Clear Data Processing Notice

This attribute assures that there is a clear Data Processing notice readily available to the user at the time(s) they need it. This attribute also ensures that the notice conveys full information surrounding the collection, use, and sharing of information.

ASSESSMENT CRITERIA	ILLUSTRATIVE CONTROLS / NOTES
1.1 Existence of Notice	*All of these controls are measured via User Experience (UX) evaluation.* *1.1.1 The notice exists. It can be contained in the Privacy Policy, Terms of Service or other UX convention, but it must exist.*
L.1.1.1.A **CCPA** = In alignment	CPRA California Privacy Rights Act, CAL. CIV. CODE §1798.130 (5); California Privacy Rights Act, CAL. CIV. CODE §1798.100 (a) CCPA California Consumer Privacy Act, CAL. CIV. CODE §1798.130 (5); California Consumer Privacy Act, CAL. CIV. CODE §1798.100 (a)
L.1.1.1.B **GDPR** = In alignment	General Data Protection Regulation [hereinafter GDPR], Art. 12(1); GDPR, Recital 39(2); GDPR, Recital 60(1)
1.2 Understandability of Notice	*1.2.1 The notice is easy to find, especially at the point of making the Me2B Commitment.*
L.1.2.1.A **CCPA** = In alignment	B-s are legally required to provide notice via a link on the same page, but there is no requirement for the notice to be on the same screen. The AG's Regulations add that the notice should be designed & presented in a way that is easy to read & understandable in a format that draws the consumer's attention. Arguably notice on the same screen is a better design/ way to present the notice that is easy to read & understandable in a format that draws the consumer's attention. Current legal requirements: business must provide notice at or before collection. Business must provide a clear and conspicuous link on their internet homepages (defined to mean any page where PI is collected) titled "Do Not Sell or Share My Personal Information or "Limit the Use of My Sensitive Personal Information" [or added by CPRA: at business' discretion utilize a single clearly labeled link in lieu of the " " above that enables user to limit the use of both. CPRA California Privacy Rights Act, CAL. CIV. CODE §1798.100 (a); California Privacy Rights Act, CAL. CIV. CODE §1798.135(a); California Privacy Rights Act, CAL. CIV. CODE §1798.121; California Consumer Privacy Act, CAL. CODE REGS. tit. 11, §999.305 CCPA California Consumer Privacy Act, CAL. CIV. CODE §1798.100 (a)
L.1.2.1.B **GDPR** = In alignment	GDPR, Art. 12(1); GDPR, Recital 39(4)

1.2 Understandability of Notice		*1.2.2 The data processing notice describes the data processing for the particular Me2B Commitment.*
L.1.2.2.A **CCPA**	↑ ISL Spec exceeds the law	Legally requires notices that break out data processing into specific categories of PI & purposes that are very broad. Categories of PI include sISLces from which consumers PI is collected; Business or commercial purpose for collecting or sharing PI; and categories of third parties to whom the Business discloses PI. CPRA California Privacy Rights Act, CAL. CIV. CODE §1798.100 (a); California Privacy Rights Act, CAL. CIV. CODE §1798.135(a); California Privacy Rights Act, CAL. CIV. CODE §1798.121; California Consumer Privacy Act, CAL. CODE REGS. Tit. 11, §999.305 CCPA California Consumer Privacy Act, CAL. CIV. CODE §1798.100 (a)
L.1.2.2.B **GDPR**	↑ ISL Spec exceeds the law	Per Article 5(1)(a), data processing must be lawful, fair, and transparent. The requirement for transparency implies accurate notice. Notice is explicitly required when the legal basis for data processing is "Consent". B-s need a data subject's consent for each specific use purpose. GDPR, Art. 13(1); GDPR, Art. 13(2); GDPR, Art. 14; GDPR, Art. 6(1); GDPR Art. 5(1)
1.2 Understandability of Notice		*1.2.3 The notice is accessible by machine readers (assistive devices).*

L.1.2.3.A **CCPA**	= In alignment	Legally requires notice to be accessible to consumers with disabilities and also available in all languages in the Business' ordinary cISLse of Business.
		CPRA California Privacy Rights Act, CAL. CIV. CODE §1798.100(a); California Privacy Rights Act, CAL. CIV. CODE §1798.135(a); California Privacy Rights Act, CAL. CIV. CODE §1798.140(p);
		CA AG California Consumer Privacy Act, CAL. CODE REGS. tit. 11, §999.301(l); California Consumer Privacy Act, CAL. CODE REGS. tit. 11, §999.301(m); California Consumer Privacy Act, CAL. CODE REGS. tit. 11, §999.301(m); California Consumer Privacy Act, CAL. CODE REGS. tit. 11, §999.301(p); California Consumer Privacy Act, CAL. CODE REGS. tit. 11, §999.304; California Consumer Privacy Act, CAL. CODE REGS. tit. 11, §999.305;

L1.2.3.B **GDPR**	= In alignment	GDPR, Art. 12(7); GDPR, Art. 21 (5); GDPR, Recital 60(5); GDPR, Recital 60(6);
1.2 Understandability of Notice		*1.2.4 The notice is complete. Notice includes minimally the following:* *- the Me2B Deal terms for the particular commitment (gives and gets)* *- how the collected information will be used*

		- what "invisible information" (behavioral information, e.g.) is collected *- how long information will be saved* *- who (what Data Processors, and specifically, company names) will receive information and what they use the information for, and how long they retain the information*
L.1.2.4.A **CCPA**	↑ ISL Spec exceeds the law	The law only requires the following: disclosure of the categories of PI & "Sensitive PI" and the purpose for which the PI was collected; and whether the PI is sold or shared. Law also requires: disclosure of how long PI is retained, the criteria to determine the period and states that Business should not retain PI or SPI for longer than reasonably necessary for the purpose. CPRA California Privacy Rights Act, CAL. CIV. CODE §1798.100(a); CCPA California Consumer Privacy Act, CAL. CIV. CODE §1798.100(a)
L.1.2.4.B **GDPR**	↑ ISL Spec exceeds the law	ISL spec aligns with EU citizen's right to be informed about the personal data that data processors collect, how it will be used, and to whom it will be transferred. However, the law allows the notice to be sufficient when recipients or "categories of recipients" are named. As such, ISL requirements are greater than what the law requires. Also, under the law, B-s need a data subject's consent for each specific use purpose… does this satisfy the Me2B deal terms or are ISL terms greater than the legal requirement? Otherwise, in alignment with the minimum notice requirements. GDPR, Art. 13(1); GDPR, Art. 13(2)
1.2 Understandability of Notice		*1.2.5 The notice clear and easy to understand by the general population.* *Readable notice copy is at grade level 6 or better (lower) with additional explainer copy at grade level 6 or better as measured by: https://www.webfx.com/tools/read-able/flesch-kincaid.html*

L.1.2.5.A **CCPA**	↑ ISL Spec exceeds the law	ISL spec aligns with the AG's vision that notice should be designed & presented in a way that is easy to read & understandable using plain, straightforward language. However, there is no mention of a test to determine understandability in the law. CA AG California Consumer Privacy Act, CAL. CODE REGS. tit. 11, §999.305; California Consumer Privacy Act, CAL. CODE REGS. tit. 11, §999.308(a)(2); California Consumer Privacy Act, CAL. CODE REGS. tit. 11, §999.308(c); California Consumer Privacy Act, CAL. CODE REGS. tit. 11, §999.315(h)(2)
L.1.2.5.B **GDPR**	↑ ISL Spec exceeds the law	GDPR does not explicitly state "by the general population" but that could be inferred by their broad definition. There are no requirements that indicate a way to measure that the language is easy to understand. As such, ISL requirement that a readable copy be made at grade level 6 or lower is better. GDPR, Art. 7(2); GDPR, Art. 4(11); GDPR, Recital 42; GDPR, Recital 39;

7 ATTRIBUTE 2: Viable Permission for Data Processing

This attribute assures that no data is collected without viable permission. We use the Nancy Kim criteria for viable permission:
(1) Understandability - the Data Subject readily understands the permissions being sought,
(2) Freely given - the Data Subject is not coerced in any way including through dark patterns, and the permission is freely given, and,
(3) Intentional action - the Data Subject provides an intentional action in order to signify permission; contracts of adhesion, for example, do not constitute intentional action.

ASSESSMENT CRITERIA		ILLUSTRATIVE CONTROLS / NOTES
2.1 Understandability of requested permission		*Controls 2.1.1 through 2.3.1 are measured via User Experience (UX) evaluation. 2.4.1 through 2.6.1 are measured through both UX evaluation and data flow analysis.* *2.1.1 The information the Data Subject receives at the point of data collection and use is sufficient to provide informed permission.*
L.2.1.1.A **CCPA**	↑ ISL Spec exceeds the law	Law mentions informed permission. This also ties into understandability concepts in Attribute 1. CPRA California Privacy Rights Act, CAL. CIV. CODE §1798.140(H)
L.2.1.1.B **GDPR**	= In alignment	GDPR, Art. 4(11)
2.2 Freely Given Permission		*2.2.1 The Data Subject freely gives permission for the requested data (uncoerced, no dark patterns in UX).*
L.2.2.1.A **CCPA**	= In alignment	The CPRA defines consent as "freely given, specific, informed, and unambiguous indication of the consumer's wishes." Also stating that agreements obtained through dark patterns do not constitute consent. CPRA California Privacy Rights Act, CAL. CIV. CODE §1798.140(L); California Privacy Rights Act, CAL. CIV. CODE §1798.140(H)
L.2.2.1.B **GDPR**	= In alignment	GDPR, Art. 4(11); GDPR, Recital 40
2.3 Intentional Action		*2.3.1 There is a required action the Data Subject must take in order to affirmatively provide permission for data processing, i.e., that data processing does not happen without the Data Subject's deliberate permission. For instance, contracts of adhesion, such as, "By continuing to use this website, you agree to ISL terms of service," do not constitute an intentional action and are unacceptable.*

L.2.3.1.A **CCPA**	🚫 Not included	Under the CPRA, it's unclear if contracts of adhesion will or will not constitute an intentional action. Definition of Consent states that “Acceptance of a general or broad terms of use, or similar document, that contains descriptions of personal information processing along with other, unrelated information, does not constitute consent.” CPRA California Privacy Rights Act, CAL. CIV. CODE §1798.140(H); California Privacy Rights Act, CAL. CIV. CODE §1798.140(S)
L.2.3.1.B **GDPR**	= In alignment	GDPR, Art. 4(11); GDPR, Art. 6(1); GDPR, Art. 7(1); GDPR, Recital 42(1); GDPR, Recital 42(5); GDPR, Recital 43
2.4 Permission Flow to Downstream Data Processors		*2.4.1 The Data Subject's permissions flow downstream to all co-Data Controllers and Data Processors. This control is measured through data flow analysis and evaluation of self-reported answers provided by the Data Controller.*
L.2.4.1.A **CCPA**	= In alignment	Data subjects permissions flow to “service providers”. CA AG California Consumer Privacy Act, CAL. CODE REGS. tit. 11, §999.314
L.2.4.1.B **GDPR**	= In alignment	GDPR, Art. 82(2); GPDR, Art. 28(1); GDPR, Art. 29; GDPR, Art.31; GDPR, Recital 81
2.5 Appropriate Control		*2.5.1 The data subject is afforded an appropriate level of control for the commitment parameters. E.g. If the service is collecting location information, depending on the nature of the service, the data subject should be given the option to share coarse- vs. fine-grained location information.*
L.2.5.1.A **CCPA**	🚫 Not included	No mention of appropriate level of control for commitment parameters.

L.2.5.1.B **GDPR**	↑ ISL Spec exceeds the law	Similar to legal requirement that consent should be given for each purpose if the processing has multiple purposes. But ISL requirements (are better) exceed the legal requirements by requiring an appropriate level of control for the commitment parameters. GDPR, Recital 43(2); GDPR, Recital 42(2)
2.6 No Data Collection Prior to Data Subject Permission		*2.6.1 The service does not collect commitment-related information prior to the data subject's explicit permission.*
L.2.6.1.A **CCPA**	↑ ISL Spec exceeds the law	The law is centered around notice at collection rather than granting of permission. B-s are legally required not to collect PI if they did not provide notice before or at time of collection. CA AG California Consumer Privacy Act, CAL. CODE REGS. tit. 11, §999.305(1); California Consumer Privacy Act, CAL. CODE REGS. tit. 11, §999.305(5); California Consumer Privacy Act, CAL. CODE REGS. tit. 11, §999.305(6)
L.2.6.1.A **GDPR**	= In alignment	GDPR requires a data subject to opt-in prior to collecting that data subject's personal data. GDPR, Art. 4; GDPR, Recital 43(2); GDPR, Recital 32

8 ATTRIBUTE 3: Identification Minimization

This attribute assures privacy protection by ensuring that the level of identification [of the Data Subject] is proportional to the stage of the Me2B Commitment.

ASSESSMENT CRITERIA		ILLUSTRATIVE CONTROLS/ NOTES
3.1 Assess whether or not the identification and data correlation performed by the data controller in the Me2B Commitment is appropriate and proportional to the Me2B Commitment.		*All of these controls are measured via data flow analysis.* *3.1.1 The identification in use reflects the stage of the Me2B Relationship, i.e., is proportional to the Me2B Commitment:* *COMMITMENT <--> IDENTIFICATION* *- None None* *- Local Storage Session ID (website); no cross-site IDs* *- Location Site + Session ID (website)* *- Promotional Comms Email* *- Customer Care Email* *- One-off Trans Unique Customer ID* *- Loyalty Program Unique Customer ID* *- Account Creation Unique Customer ID* *See also Figure 4 below.*
L.3.1.1.A **CCPA**	🚫 Not included	
L.3.1.1.B **GDPR**	↑ ISL Spec exceeds the law	Similar to the legal requirement that personal data be "kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed." GDPR, Art. 5 (1)(e)

3.2 Assess whether or not the identification and data correlation performed by downstream co-data controllers and data processors is appropriate and proportional to the Me2B Commitment and Me2B Deal.	*3.2.1 Data subject identification comports to appropriate state of Me2B Lifecycle, and the data subject "joinkey" isn’t used to correlate behavioral data in an expected way by data processors & co-controllers. Data subject is not being actively tracked beyond the expected scope of this commitment per the Me2B Lifecycle.*
L.3.2.1.A **CCPA**	🚫 Not included
L.3.2.1.B **GDPR**	🚫 Not included

Attribute 3: Identification Minimization - Me Experience

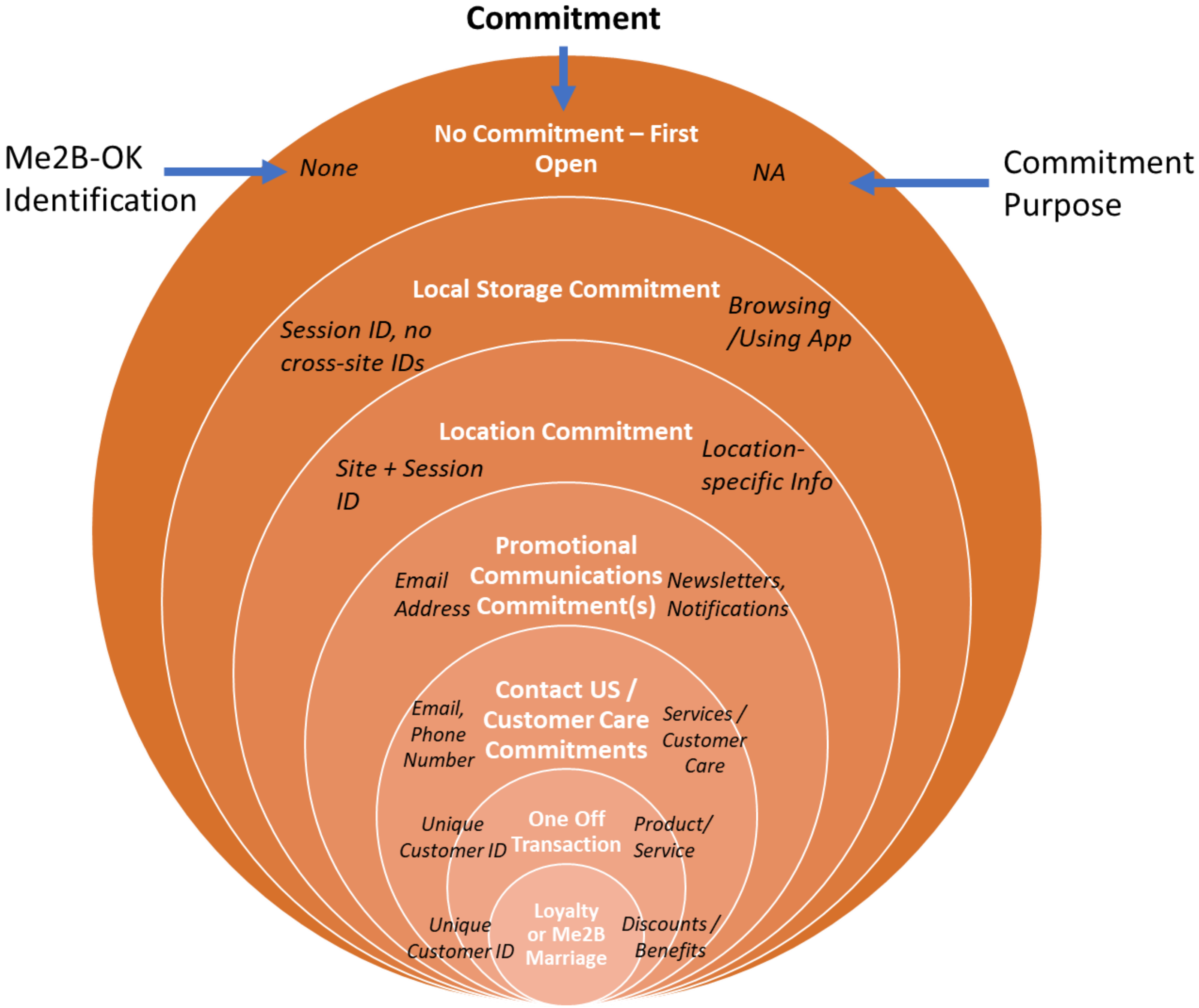

Figure 4 Identification Minimization

9 ATTRIBUTE 4: Data Collection Minimization

This attribute assures that only the minimum amount of information is collected in order to provide the promised service.	
ASSESSMENT CRITERIA	**ILLUSTRATIVE CONTROLS/ NOTES**
4.1 Assess whether the data being collected for the Me2B Commitment is reasonable for the Me2B Commitment.	*4.1.1 Each Me2B Commitment has a context-sensitive list of acceptable minimal data. Refer to Figure 5 for illustrative data collection minimization per Me2B Commitment. More details can be found in the detailed specification. (Measured via UX analysis.)*
L.4.1.1.A **CCPA** 🚫 Not included	
L.4.1.1.B **GDPR** 🚫 Not included	

4.1 Assess whether the data being collected for the Me2B Commitment is reasonable for the Me2B Commitment.		*4.1.2 Information volunteered by the data subject is appropriate for the particular Me2B Commitment.*
L.4.1.2.A **CCPA**	🚫 Not included	
L.4.1.2.B **GDPR**	= In alignment	Legally requires that the personal data collected be “adequate, relevant, and limited to what is necessary” to the specific purpose for which the data is being processed. GDPR Art.5(1)(c); GDPR, Art. 25; GDPR, Recital 156.
4.1 Assess whether the data being collected for the Me2B Commitment is reasonable for the Me2B Commitment.		*4.1.3 Information observed by the data controller via data subject interaction is appropriate for the particular Me2B Commitment.*
L.4.1.3.A **CCPA**	🚫 Not included	Regulations from Attorney General make inferences about Data minimization. Stating that Businesses are not obligated to provide or delete data if they maintain deidentified data. CA AG California Consumer Privacy Act, CAL. CODE REGS. tit. 11, §999.323(f); California Consumer Privacy Act, CAL. CODE REGS. tit. 11, §999.306(d); California Consumer Privacy Act, CAL. CODE REGS. tit. 11, §999.313(c)(3);
L.4.1.3.B **GDPR**	🚫 Not included	

4.1 Assess whether the data being collected for the Me2B Commitment is reasonable for the Me2B Commitment.	*4.1.4 Information derived by the data controller is appropriate for the particular Me2B Commitment.*
L.4.1.4.A **CCPA**	🚫 Not included
L.4.1.4.B **GDPR**	🚫 Not included

Attribute 4: Data Collection Minimization

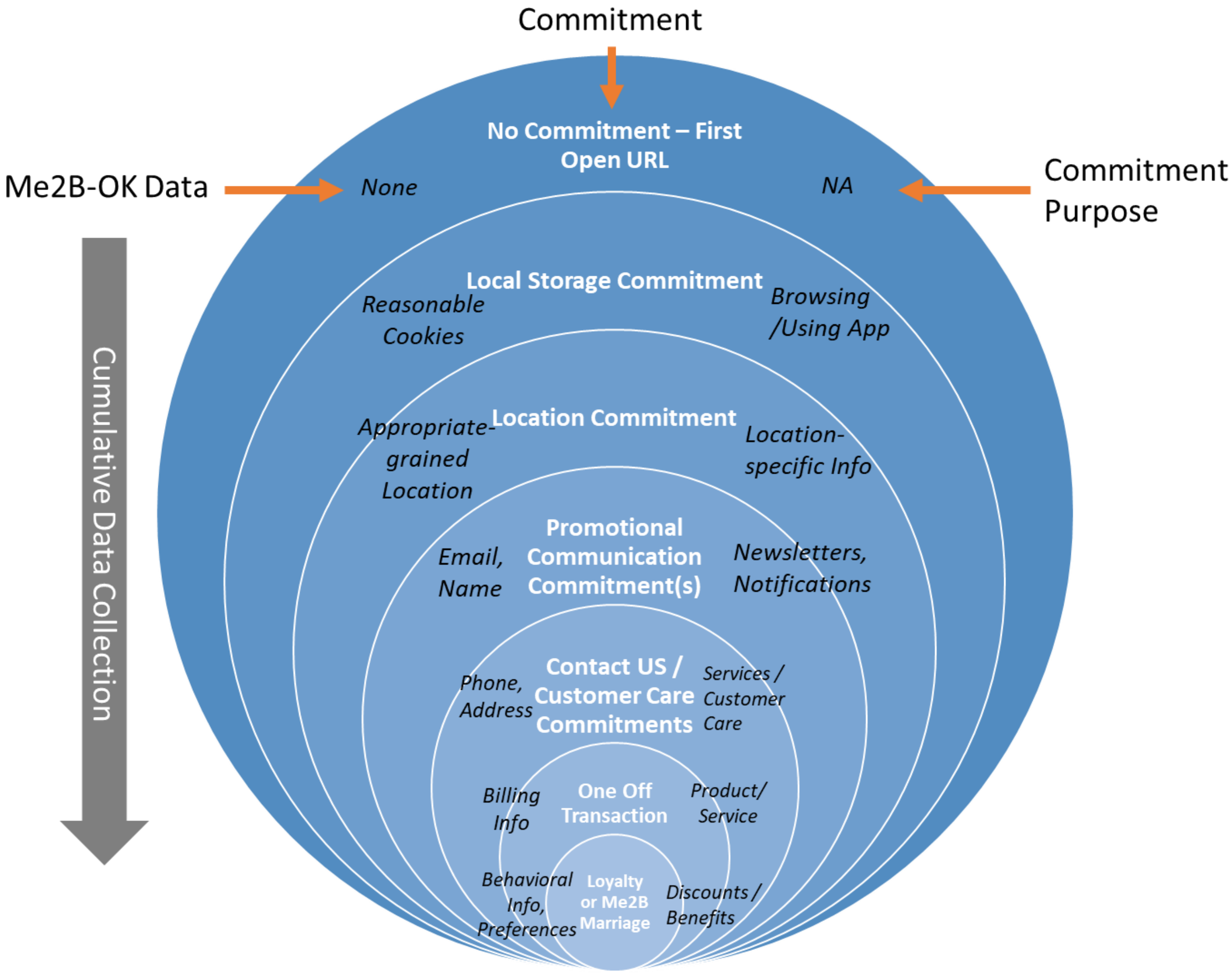

Figure 5 Data Collection Minimization per Commitment

10 ATTRIBUTE 5: Private by Default

This attribute assures that the service (software) always defaults to the most conservative privacy settings and behaviors available, and that the Data Subject does not need to take any additional action in order to have a private experience.

ASSESSMENT CRITERIA		ILLUSTRATIVE CONTROLS/ NOTES
5.1 Assess whether the information shared for the Me2B Commitment is automatically private by default, or if the Data Subject has to adjust settings in order to ensure privacy.		*5.1.1 Each time the Data Subject enters a Me2B Commitment, no additional action is required in order to have a private experience. If there are privacy settings relating to the commitment, they default to the most private settings. (This control is measured via UX evaluation.)* *5.1.2 Network traffic is evaluated in order to ensure that data isn't being automatically shared with Data Processors or co-Data Controllers in an inappropriate way. (This control is measured via data flow analysis as part of Attribute 6.)*
L.5.1.A **CCPA**	🚫 Not included	The CCPA and CPRA both contain a major deviation from this ISL safety requirement: there is no requirement for service providers to be private by design, and in fact, the regulation tacitly supports share by design as a default, given how the Do Not Sell/Share My Data capability is defined.
L.5.1.B **GDPR**	↑ ISL Spec exceeds the law	GDPR has a privacy by design and default philosophy. B-s must implement appropriate measures (at the time of the determination of the means for processing and at the time of the processing itself) to ensure that by default they are only collecting the personal data that is necessary for each specific purpose of the processing. GDPR, Art. 25

11 ATTRIBUTE 6: Reasonable Data Use & Sharing Behavior

Similar to attributes 3 and 4, reasonable data use and sharing behavior is proportional to the Me2B Commitment under evaluation. This attribute assures that the data use and sharing behavior is proportional and appropriate to the particular Me2B Commitment.

ASSESSMENT CRITERIA		ILLUSTRATIVE CONTROLS/ NOTES
6.1 Assess whether the collected data is being used in an expected and reasonable way.		*These controls are primarily measured via data flow analysis and evaluation of self-reported answers provided by the Data Controller.* *6.1.1 Data Controller supplied information (questionnaire) matches observed data use behavior for the commitment.* *6.1.2 The UX doesn't indicate any unexpected (spurious) use of collected data. (This is determined by UX evaluation.)*
L.6.1.A **CCPA**	🚫 Not included	Business use shall be reasonably necessary and proportionate to achieve the purpose for which PI was collected or processed. PI should not be processed in an incompatible manner. CPRA California Privacy Rights Act, CAL. CIV. CODE §1798.100(c); California Privacy Rights Act, CAL. CIV. CODE §1798.140(e)
L.6.1.B **GDPR**	= In alignment	Discussed in the GDPR's supervising agencies guidance (EDPB and ICO). The law requires lawful processing meaning that data should only be processed/collected if the data subject gave consent or if it is necessary for another reason. When processing is not necessary for the performance of the contract, the processing can only take place if it relies on another appropriate legal basis. To determine what is 'necessary' enforcers will conduct a fact-based assessment of the processing "for the objective pursued and of whether it is less intrusive compared to other options for achieving the same goal". If there are less intrusive alternatives available then the processing is not 'necessary'. Processing that is useful but not objectively necessary for performance is not lawful, even if it is necessary for the controller's other business purposes. GDPR Art. 6; GDPR, Art. 24(1)

6.2 Assess whether the Data Controller is reasonably sharing collected information with 3rd party co-data Controllers or Data Processors		*6.2.1 Data Controller supplied information validates that collected data is only being shared with co-Data Controllers and Data Processors involved in fulfilling the commitment-specific services.* *6.2.2 Data flow analysis validates that data is only being shared with Co-Data Controllers and Data Processors involved in fulfilling the commitment-specific services.*
L.6.2.A **CCPA**	↑ISL Spec exceeds the law	Business has a legal limitation to share PI for limited specified purposes (Business's operational purpose or co-controller's operational purpose). Co-controllers are prohibited from retaining, using, sharing, selling info for any purpose other than the purpose specified. Cross contextual behavioral advertising is explicitly called out as not being an ad/marketing service that is an operational purpose. No specific mention of join keys. CPRA California Privacy Rights Act, CAL. CIV. CODE §1798.100(d); California Privacy Rights Act, CAL. CIV. CODE §1798.140(e); California Privacy Rights Act, CAL. CIV. CODE §1798.140(ag); CA AG California Consumer Privacy Act, CAL. CODE REGS. tit. 11, §999.314(c)
L.6.2.B **GDPR**	↑ISL Spec exceeds the law	The law requires a contract between the controller and the co-data controller and sets out series of requirements for these contracts. Data controllers shall only use co-data controllers that provide sufficient guarantees to implement appropriate technical and organizational measures. GPDR, Art. 28; GDPR, Art. 29; GDPR, Art.31; GDPR, Recital 81

6.3 Assess whether the level of data sharing is on par with industry norms.	*6.3.1 Data sharing is equal or less than (better) than industry norms using the Me2BA industry benchmarks for similar services.*
L.6.3.A **CCPA**	🚫 Not included
L.6.3.B **GDPR**	🚫 Not included

12 ATTRIBUTE 7: Data Processing Matches Data Subject's Permissions & Preferences

This attribute assures that the observed data processing matches the Data Subject's permissions and preferences.

ASSESSMENT CRITERIA		ILLUSTRATIVE CONTROLS/ NOTES
7.1 Assess whether or not the observed data processing (collection, use and sharing) matches the Data Subject's asserted preferences and permission.		*All of these controls are measured via data flow analysis.* *7.1.1 The observed data collection comports with the Data Subject's permissions & preferences.*
L.7.1.1.A **CCPA**	🚫 Not included	Legal violation may arise if a B shares Me's collected data after Me opts out. CPRA California Privacy Rights Act, CAL. CIV. CODE §1798.100(a)(1); California Privacy Rights Act, CAL. CIV. CODE §1798.100(a)(c); California Privacy Rights Act, CAL. CIV. CODE §1798.145(i)(2);
L7.1.1.B **GDPR**	⊘ Not included, inferred	Practically required by requirement for consent before data collection. While these details are not expressly mentioned in the law, for data controllers to lawfully process data (if the processing does not fall under any other category in Article 6) they must have the data subject's consent meaning that they must comport with their permissions & preferences, *in theory*. Valid consent is discussed in more detail in Attribute 2. GDPR, Art. 4(11); GDPR, Art. 6(1); GDPR, Art. 7(1); GDPR, Recital 42(1); GDPR, Recital 42(5); GDPR, Recital 43
7.1 Assess whether or not the observed data processing (collection, use and sharing) matches the Data Subject's asserted preferences and permission.		*7.1.2 The observed data controller data use and sharing comports with the Data Subject's permissions & preferences.*
L7.1.2.A **CCPA**	🚫 Not included	
L7.1.2.B **GDPR**	🚫 Not included	

7.1 Assess whether or not the observed data processing (collection, use and sharing) matches the Data Subject's asserted preferences and permission.	*7.1.3 The observed data processor and co-data controller use and sharing comports with the Data Subject's permissions and preferences.*
L7.1.3.A **CCPA**	🚫 Not included
L7.1.3.B **GDPR**	🚫 Not included

13 ATTRIBUTE 8: Data Processing Matches Notices/Policies

This attribute assures that the observed data processing matches what is stated in the Data Controller's Privacy Policy and Terms of Service.

ASSESSMENT CRITERIA		ILLUSTRATIVE CONTROLS/ NOTES
8.1 Assess whether the observed data processing (collection, use, and sharing) matches the Privacy Policy and Terms of Service.		*These controls are measured by comparing the observed data processing behavior (UX and data flow analysis) to the promised data processing as described in the Data Controller's Privacy Policy and Terms of Service.* *8.1.1 The observed data collection matches what's stated in the Privacy Policy. (Measured via UX analysis.)*
L.8.1.1.A **CCPA**	⊘ Not included, inferred	Readily inferable. Law does not explicitly state that the observed data match provided notices but it can easily be inferred from their rule language. CPRA California Consumer Privacy Act, CAL. CODE REGS. tit. 11, §999.305(6); California Privacy Rights Act, CAL. CIV. CODE §1798.130 (5); California Privacy Rights Act, CAL. CIV. CODE §1798.100 (a); CCPA - California Consumer Privacy Act, CAL. CIV. CODE §1798.130 (5); California Consumer Privacy Act, CAL. CIV. CODE §1798.100 (a)
L.8.1.1.B **GDPR**	⊘ Not included, inferred	Readily inferable. Law does not go into this detail but there is a strong argument that this could be inferred. Because if B-s collect and use any additional personal data than what the data subject originally consented to the B-s would be required to get the data subject to consent to that new collection/use. GDPR, Art. 6(1); GDPR, Art. 7; GDPR, Art. 13(1); GDPR, Art. 13(2); GDPR, Art. 14; GDPR, Recital 42; GDPR, Recital 43
8.1 Assess whether the observed data processing (collection, use, and sharing) matches the Privacy Policy and Terms of Service.		*8.1.2 The observed data collection matches what's stated in the Terms of Service. (Measured via UX analysis.)*
L.8.1.2.A **CCPA**	⊘ Not included	
L.8.1.2.B **GDPR**	⊘ Not included	

8.1 Assess whether the observed data processing (collection, use, and sharing) matches the Privacy Policy and Terms of Service.	*8.1.3 The observed data use matches what's stated in the Privacy Policy. (Measured via UX and data flow analysis.)*
L.8.1.3.A **CCPA**	🚫 Not included
L.8.1.3.B **GDPR**	🚫 Not included
8.1 Assess whether the observed data processing (collection, use, and sharing) matches the Privacy Policy and Terms of Service.	*8.1.4 The observed data use matches what's stated in the Terms of Service. (Measured via UX and data flow analysis.)*
L.8.1.4.A **CCPA**	🚫 Not included
L.8.1.4.B **GDPR**	🚫 Not included
8.1 Assess whether the observed data processing (collection, use, and sharing) matches the Privacy Policy and Terms of Service.	*8.1.5 The observed data sharing matches what's stated in the Privacy Policy. (Measured via data flow analysis.)*
L.8.1.5.A **CCPA**	🚫 Not included
L.8.1.5.B **GDPR**	🚫 Not included
8.1 Assess whether the observed data processing (collection, use, and sharing) matches the Privacy Policy and Terms of Service.	*8.1.6 The observed data sharing matches what's stated in the Terms of Service. (Measured via data flow analysis.)*
L.8.1.6.A **CCPA**	🚫 Not included
L.8.1.6.B **GDPR**	🚫 Not included

14 ATTRIBUTE 9: Reasonable Commitment Duration

This attribute assures that commitment duration is appropriate for the particular commitment.	
ASSESSMENT CRITERIA	ILLUSTRATIVE CONTROLS/ **NOTES**
9.1 Assess whether the observed Me2B Commitment duration (default) is appropriate for the Me2B Commitment.	*9.1.1 Default duration for the commitment is appropriate for the commitment:* *COMMITMENT <--> DEFAULT DURATION* *- None — NA* *- Local Storage — Session duration* *- Location — Session Duration* *- Contact Us — Until the reason for contact has been completely fulfilled* *- Promotional — Until Data Subject or Data Controller Terminates* *- One-off Trans — As long as Data Controller legal obligations require* *- Loyalty Program — Until Data Subject or Data Controller Terminates* *- Account Creation — Until Data Subject or Data Controller Terminates* *This control is measured via UX and data flow analysis.*
L.9.1.A **CCPA** ↑ISL Spec exceeds the law	The law states that PI or SPI should not be retained for longer than reasonably necessary for the purpose. But the law does not clarify what it considers reasonable. CPRA California Privacy Rights Act, CAL. CIV. CODE §1798.100 (a)(3)
L.9.1.B **GDPR** ↑ISL Spec exceeds the law	Similar to the legal requirement to not store data subject's personal data for longer than is necessary for the specific purposes for which the data is processed. B-s should ensure that the personal data is not kept longer than necessary by establishing time limits for erasure or for a periodic review. B-s should also provide the duration of their data collection in their notice or provide the criteria used to determine that duration period. GDPR, Art. 5(e); GDPR, Recital 39(10)

15 ATTRIBUTE 10: Commitment Termination Behavior

This attribute assures that the Data Subject can readily terminate commitments and that commitment termination behavior properly deletes any data and essentially "forgets" the Data Subject.

ASSESSMENT CRITERIA		ILLUSTRATIVE CONTROLS/ **NOTES**
10.1 Assess the UX to determine if it's easy for the Data Subject to stop the Me2B Commitment.		*10.1.1 The Data Subject can easily stop the Me2B Commitment. (Measured by UX analysis.)*
L.10.1.1.A **CCPA**	🚫 Not included	
L.10.1.1.B **GDPR**	🚫 Not included	Not exactly a Me2B Commitment but the GDPR does provide Data Subjects with the right to object to data processing at any time. Essentially, a Data Subject can restrict Data Controller's from processing their personal data when: (1) they object to the data processing; (2) they contest the accuracy of the personal data; or (3) the processing is unlawful. GDPR, Art. 21; GDPR, Art. 18
10.2 Assess if the Data Subject receives a record of the change or termination of the Me2B Commitment.		*10.2.1. The Data Subject receives a record of the termination of the Me2B Commitment. (Measured by UX analysis.)*
L.10.2.A **CCPA**	↑ ISL Spec exceeds the law	Law does not require a record for termination of all commitments. B-s must reply to request to know or request to delete. CCPA California Consumer Privacy Act, CAL. CODE REGS. tit. 11, §999.313(a); California Consumer Privacy Act, CAL. CODE REGS. tit. 11, §999.313(b); California Consumer Privacy Act, CAL. CODE REGS. tit. 11, §999.313(d)(4); California Consumer Privacy Act, CAL. CODE REGS. tit. 11, §999.313(d)(5); California Consumer Privacy Act, CAL. CODE REGS. tit. 11,§999.316(c)
L.10.2.B **GDPR**	🚫 Not included	The law does not require a record of the termination of all commitments. B-s are legally required to provide information to data subject within 1 month of the data subject's request to: access; rectify; erase; restrict processing. GDPR, Art. 12(3)(1)

10.3 Assess whether the Data Controller removes all collected data upon termination of the Me2B Commitment (as appropriate for the particular commitment and legal/tax requirements).		*10.3.1 The Data Controller removes all collected data upon termination of the Me2B Commitment (except for data legally required to retain). (Measured by data flow analysis and UX analysis.)*
L.10.3.A **CCPA**	↑ ISL Spec exceeds the law	The law only requires the data controller to remove or change data upon a consumer's request to delete information…some exceptions do apply. CPRA California Privacy Rights Act, CAL. CIV. CODE §1798.105(a); California Privacy Rights Act, CAL. CIV. CODE §1798.105(c)(1); California Privacy Rights Act, CAL. CIV. CODE §1798.105(c)(3); California Consumer Privacy Act, CAL. CODE REGS. tit. 11, §999.313(d)(2); California Consumer Privacy Act, CAL. CODE REGS. tit. 11, §999.313(8); California Consumer Privacy Act, CAL. CODE REGS. tit. 11, §999.314; *See* California Privacy Rights Act, CAL. CIV. CODE §1798.105(d) for exceptions.
L.10.3.B **GDPR**	= In alignment	GDPR, Art. 17; GDPR, Art. 19; GDPR, Recital 39(11); GDPR, Recital 65; GDPR, Recital 66

10.4 Assess whether all downstream co-Data Controllers and Data Processors both receives and properly respond to changes to and termination of the Me2B Commitment.		*10.4.1 All downstream co-Data Controllers and Data Processors receive notification that the Me2B Commitment has been terminated. (Measured via data flow analysis.)* *10.4.2 All downstream co-Data Controllers and Data Processors delete Data* *Subject's data (except for data legally required to retain). (Measured via data flow analysis and self-reported information from Data Controller.)*
L.10.4.A **CCPA**	↑ ISL Spec exceeds the law	For requests to delete the law requires notification to all service providers, contractors and third parties ("unless this proves impossible or involves disproportionate effort"). CPRA California Privacy Rights Act, CAL. CIV. CODE §1798.105(c)(1); California Privacy Rights Act, CAL. CIV. CODE §1798.105(c)(3); *See also* California Privacy Rights Act, CAL. CIV. CODE §1798.145(i); California Consumer Privacy Act, CAL. CIV. CODE §1798.145(i); California Privacy Rights Act, CAL. CIV. CODE §1798.145(j)(1)
L.10.4.B **GDPR**	= In alignment	All data controllers must delete Data Subject's personal data and notify co-controllers. B-s are legally required to communicate "any rectification or erasure of personal data or restriction of processing carried out to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort." GDPR, Art. 19; GDPR, Art. 18(2); GPDR, Art. 28(3)(g); GDPR, Art.31;GDPR, Recital 81

Appendix A: Regulation Terminology Mapping

ISL Language Used	CCPA/CPRA	GDPR
Data Subject	**“Consumer”**	**“Data Subject”**
Data Controller	**“Business”**	**“Data Controller”**
Data Processor	**“Service Providers”** and **“Contractors”** *both added by CPRA	**“Data Processor”**
Data Co-Controller	🚫 Not Included	**“Joint Controller”**
Data	**“Personal Information”**	**“Personal Data”**
Data Broker	**“Third Party”**	**“Third Party”**