INTERNET SAFETY LABS

ISL Safe Software Specification
Websites and Mobile Apps
Core Requirements

Version 1.1
RTS WG
05-Jul-22

VERSION	DATE	PLATFORMS	EDITORS	CONTRIBUTORS	DESCRIPTION OF CHANGES
0.1	08/21/21	Websites	L. LeVasseur	RTS WG	Candidate Working Group Approval draft
0.2	10/10/21	Websites	L. LeVasseur	RTS WG	WG Approved Draft
0.7	12/28/21	Websites, Mobile Apps	L. LeVasseur	RTS WG	Simplified after lack of comments in two review periods.
1.0	04/26/22	Websites, Mobile Apps	L. LeVasseur	RTS WG	Publication version.
1.05	04/30/22	Websites, Mobile Apps	L. LeVasseur, Daniella Doern	L. LeVasseur, Daniella Doern	Added CPRA and GDPR Mapping
1.06	06/06/22	Websites, Mobile Apps	L.LeVasseur	L. LeVasseur, Daniella Doern	Changed name of Me2B Marriage Commitment commitment; and organization name.
1.1	07/05/22	Websites, Mobile Apps	L. LeVasseur, Daniella Doern	L. LeVasseur, Daniella Doern	Publication version.

This workbook constitutes the ISL Safe SW Specification Core Requirements for Websites and Mobile Apps.

CONTRIBUTORS

The following individuals have participated in the Respectful Tech Spec Working Group since its inception in April 2019:

James Aschberger	Zach Edwards	Corey Jackson	Michele Silverthorn
Andrea Ausland	Guy Gabriele	Lisa LeVasseur	Shaun Spalding
Ted Barthell	Cam Geer	Camille Nebeker	Jay VanBuren
Justin Byrd	Jane Gould	Kelsey Nordstrom	Richard Whitt
Haley Dahlberg	Iain Henderson	Jeff Orgel	Noreen Whysel
Daniella Doern	Mary Hodder	Jim Pasquale	John Wunderlich

The following individuals are voting members in the Respectful Tech Spec WG at the time of publication of this specification v1.0, April 29, 2022:

Justin Byrd
Haley Dahlberg
Zach Edwards
Mary Hodder
Lisa LeVasseur
Jeff Orgel
Jim Pasquale
Noreen Whysel
John Wunderlich

The following individuals are voting members in the Software Safety Standard Panel at the time of publication of this specification v1.1, July 5, 2022:

Justin Byrd
Zach Edwards
Mary Hodder
Jeff Orgel
Jim Pasquale
Noreen Whysel
John Wunderlich

1 - Software Safety Specification for Websites and Mobile Apps - Introduction

How to use this Workbook

As a website provider/maker and data controller, you can use the Website Rubric to evaluate your own websites, by running each test on your own prior to applying for a Safety Audit.

It is STRONGLY suggested that you familiarize yourself with the Me2B 101 series of Flash Guides that can be found here: https://me2ba.org/library/#flashguides

Please refer to the Internet Safety Labs Glossary also for terminology. https://me2ba.org/library/glossary/

There are data collection templates for the website audit.

In applying for a safety audit, you will be required to complete the Data Controller Questionnaire.

How to Scope a Website Safety Audit:

When performing a Website Safety Audit, the Auditor and the data controller will agree on the scope of the audit, and specifically which pages will be tested. The Auditor will prioritize pages based on:
- Page reach
- Sensitivity context of page,

An audit should cover minimally 5-7 pages, but varies depending on the size and nature of the website.

The Auditor shall first identify all of the Me2B Commitments that appear on the selected webpages.
The Audit shall consist of the following tests:

All of the tests on the "All Commitments" tab,

The "Per Commitment" tests shall be run for each Me2B Commitment found in the selected webpages (see list of Me2B Commitments below), and

The "Location Commitment" specific tests found on the "Location Specific Commitment" tab.

The "Account Creation Commitment" specific tests found on the "Account Creation Commitment Specific Commitment" tab.

How to Scope a Mobile App Safety Audit:

When performing a mobile app Safety Audit, the Auditor and the data controller will agree on the scope of the audit, and specifically which UX flows & "pages" of the app will be tested. The Auditor will prioritize flows based on trying to cover all of the Me2B Commitments that exist in the app.

The Auditor shall first identify all of the Me2B Commitments that appear in the app.
The Audit shall consist of the following tests:

- All of the tests on the "All Commitments" tab,
- The "Per Commitment" tests shall be run for each Me2B Commitment found in the app (see list of Me2B Commitments below),
- The "Location Commitment" specific tests found on the "Location Specific Commitment" tab.
- The "Account Creation Commitment" specific tests found on the "Account Creation Commitment Specific Commitment" tab.

List of Me2B Commitments

- First open / no commitment
- Local Storage Commitment -- covering cookies and all local storage.
- Location Commitment
- Promotional Communication Commitment
- One-off Transaction Commitment
- Contact Us Commitment
- Loyalty Program Commitment
- Account Creation ("Me2B Marriage") Commitment

2 - REQUIREMENTS FOR ALL COMMITMENTS

TEST #	Me2B COMMITMENT	WHAT'S BEING MEASURED		GDPR MAP		CPRA MAP	DATA USED TO MEASURE	EXPERTISE NEEDED TO EVALUATE	BEST PRACTICE (SCORE = +1)	PASSING BEHAVIORS (SCORE = 0)	FAILING BEHAVIORS (SCORES -1 to -3)
Test Scope: These tests apply to the overall service and are independent of the Me2B Commitments that appear in the service.											
AL1	*ALL*	Does data controller use the IAB's transparency and consent framework (TCF)?	🚫	Not Included	🚫	Not Included	Data Controller Questionnaire	Data supply expert	NA	Do NOT use the IAB's TCF. (TCF should stop generating an ID and sharing it, and every org that receives an ID, it's a version of the ID.) Or use the IAB's TCF and make sure that the data processors support opting out https://optout.aboutads.info/?c=2&lang=EN	Use of the IAB's TCF (-1), and data processors don't support opting out (-3)
AL2	*ALL*	Data controller use of information from data brokers.	🚫	Grey Area. See Art.6(4).	🚫	Not Included	Data Controller Questionnaire	Data supply expert	NA	data controller uses data broker obtained info for identifying known bad emails.	-3 == data controller uses data broker-obtained info for marketing, customer acquisition, advertising.
AL3	*ALL*	Data controller selling or sharing information with data brokers.	↑	Art.5; Art.21; B can sell/share after receiving Me's consent. Me has right to object to processing at anytime.	↑	1798.100; B can sell/share but must provide notice 1st.	Data Controller Questionnaire	Data supply expert	NA	No use of data brokers.	-3 == data controller sends data to at least one known data brokers.
AL4	*ALL*	Whether data subject can request and receive a copy of Personal Data (definitions per GDPR Article 4 (1), and Article (15)) including data provided/input by the data subject, observed, derived, and purchased information about the data subject.	=	Art.4(1); Art.15; Me can request info. Behavioral information could fall under the automated decision-making prong that includes profiling, and requires information on "the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject."	↑	1798.110; Me can request info but B's do not need to provide behavioral info.	Observed UX	UX Expert	NA	data subject can easily request a copy of Personal Data (definitions per GDPR Article 4 (1) and Article 15), and receives an electronic copy of all Personal Data including behavioral information within 30 days, in a format that is easy for the individual to understand.	-3 == No way for data subject to request copy of Personal Data, or data subject requested Personal Data but never received.
AL5	*ALL*	Whether data subject can request changes to Personal Data.	=	Art. 16; Yes	=	1798.106; Me can correct inaccurate data	Observed UX	UX Expert	NA	data subject can easily request changes to Personal Data and the changes take place within 30 days.	-3 == Either No ability for data subject to request changes to Personal Data, or data subject requested changes never took place.
AL6	*ALL*	Whether data subject can request to have Personal Data deleted.	=	Art.17; Yes.	=	1798.105; Yes.	Observed UX	UX Expert	NA	data subject can easily request to have Personal Data deleted and the changes take place within 30 days.	-3 == Either no ability for data subject to request deletion of Personal Data, or data subjected requested deletion but it was never deleted.
AL7	*ALL*	Whether the privacy policy is for the actual data controller (business)?	🚫	Not included	🚫	Not Included	Privacy Policy	Analyst	NA	If the privacy policy is for the actual data controller (business).	-3 == Privacy policy is not for the actual data controller
AL8	*ALL*	Whether the terms of service policy is for the actual data controller (business)?	🚫	Not Included	🚫	Not Included	Terms of Service Policy	Analyst	NA	If the terms of service policy is for the actual data controller (business).	-3 == Terms of service policy is not for the actual data controller
AL9	*ALL*	Service's use of advertising/ad related local storage.	🚫	Not Included	🚫	Not Included	Observed UX	UX expert	NA	Opt in consent to agree to personalized ads. Before consent, only contextual ads.	Personalized ads appear on website without consent. (-3)
AL10	*ALL*	If the service uses Facebook advertising.	🚫	Not Included	🚫	Not Included	Observed raw data	Data supply expert	NA	Not sharing with Facebook	Sharing with Facebook (-3)
AL11	*ALL*	If the service uses Google advertising.	🚫	Not Included	🚫	Not Included	Observed raw data	Data supply expert	NA	Not sharing with Google	Sharing with Google (-3)
Test Scope: this series of tests are performed on the information security controls/maturity of the product's and organization's identity, data protection, encryption, and security assessment/testing											
SE1	*All*	Whether personnel collecting, utilizing, and responsible for safeguarding sensitive/regulated data are briefed and trained	=	Art. 47(2)(n); Art.24(1); Art.32; B's workforce that is involved in data processing must be trained.	🚫	Not Included but see 1798.100(e) below.	Data Controller Questionnaire; Summary results from Pre-Certifications mentioned in Column H.	Security Expert	**NIST Cybersecurity Framework (CSF)** Protect: PR.AT- 1, PR.AT-2, PR.AT- 3, PR.AT- 4 / **NIST SP 800-53 Rev.5** AT-3, PM-13, SA-9, SA-16/ **HITRUST** Control Category 01.c, 02c, 13.b/ **PCI DSS Requirement** 6, 9 / **FFIEC** Domain 1 Cyber Risk Management and Oversight - Strategies&Policies, Training/ **ISO 27001:2013** A.6.1.1, A.7.2.1, A.7.2.2	Organization provides annual, and as mandated, training to applicable internal/contracted audit, privacy, information/cyber security and legal personnel in relation to data protection and privacy regulatory and compliance mandates.	-3== Organization has not met regulatory mandate to train personnel collecting, utilizing, and responsible for safeguarding sensitive/regulated data -2 == No awareness and training program defined per best/leading practices -1== Identified personnel not required to receive/report completed training
SE2	*All*	The capability and implemented security controls to securely provide access and to create, manage, and authenticate one's identity.	↑	Art. 32; But it is very broad	↑	1798.130; 999.323	Data Controller Questionnaire; Summary results from Pre-Certifications mentioned in Column H.	Security Expert	**NIST Cybersecurity Framework (CSF)** ID.GV-4, PR.AC-1, PR.AC4, PR.AC-5, PR.AC-6, PR.AC-7 / **NIST SP 800-53 Rev.5** 4 AC-1, AC-2, AC-3, AC-5, AC-6, AC-7, AC, 12, AC-14, AC-16, AC-20, AC-24, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11 PM-3, SA-2/ **HITRUST** Control Category 01.a, 01.c, 01.d, 01.e, 01.q, 01.u, 02.h, 02.i, 13.s /**PCI DSS Requirement** 2, 3, 4, 6, 7, 8, 10/**FFIEC** Domain 1 Cyber Risk Management - Audit, Domain 3 Cybersecurity Controls - Infrastructure Management, Access and Data Management, Anomalous Activity Detection, Domain 5 Cyber Incident Management and Resilience - Detection, Response and Mitigation, Escalation and Reporting/ **ISO 27001:2013** A.6,A.7, A.9, A.11, A.13	Organization/product provides a secure process to create, store, and authenticate one's identity by utilizing secure communication/data transfer of credentials and securely storing Personally Identifiable Information (PII).	-3==Personally Identifiable Information (PII) entered by user is captured/stored in plain text -2==Passwords (PWs) are generated/captured/stored in plain text -1==Product does not offer secondary factor (2FA) for authentication.
SE3	*All*	The compliance and technical capability to protect sensitive or regulated data	↑	Art. 32	↑	1798.100(e); B's shall implement reasonable security procedures and practices appropriate to the nature of the PI.	Data Controller Questionnaire; Summary results from Pre-Certifications mentioned in Column H.	Security Expert	**NIST Cybersecurity Framework (CSF)** Protect: ID.GV 3, ID.GV-4, PR.DS- 1, PR.DS-2, PR.DS-3, PR.DS-5, PR.DS-7, PR.IP-6, PR.IP-12/ **NIST SP 800-53 Rev.5** AC-4, AC-5, MP-6, PE-19, PM-3, SC-8, SI-2, SI-4/ **HITRUST** Control Category 06.d, 0.6f, 0.9aa, 13.j,13.k, 13.q/ **PCI DSS Requirement** 3, 9, 10 / **FFIEC** Domain 1 Cyber Risk Management and Oversight - IT Asset Management, Audit; Domain 3 Cybersecurity Controls - Access and Data Management, Event Detection; Domain 4 External Dependency Management - Connections, Contracts; Domain 5 Cyber Incident Management and Resilience, Planning, Testing, Detection /**ISO 27001:2013** A.6, 7, 8, 9, 10, 11, 13, 14, A.16.1.6, Clause 9, Clause 10	Sensitive/regulated data is managed and protected in accordance with applicable regulatory mandates and compliance (e.g. GDPR, CCPA, PIPDEA, GLBA, etc.). Sensitive/regulated data should be safeguarded (encrypted or tagged/classified) to negate or minimize harm caused by data breaches/leakage).	-3== Verified successful data breach incident (<180 days or unresolved) -2== External Regulator/Auditor "data protection" material weakness noted -1== Absence of data protection policies or programs
SE4	*All*	Whether encryption standards/protocols are employed as data and information are entered (ingested), handled, processed, stored, or presented	🚫	Not expressed in Art. 25 but it could be inferred to be privacy by design.	↑	1798.150; Me's whose nonencrypted PI is subject to unauthorized disclosure may take civil action.	Data Controller Questionnaire; Summary results from Pre-Certifications mentioned in Column H.	Security Expert	**NIST Cybersecurity Framework (CSF)** Protect: PR.PT-2, PR.PT-4, PR.DS- 1, PR.DS-2, PR.DS-3, PR.DS-5/ **NIST SP 800-53 Rev.5 AC-4,** SC-8, SC-11, SC-12, SC-13, SC-20, SC-21, SC-22, SC-23, SC-28, SC-38, SC-31, SI-4/ **HITRUST** Control Category 06.d, 10.f/ **PCI DSS Requirement** 1, 3, 4, / **FFIEC Domain** 3 Cybersecurity Controls Access and Data Management/ **ISO 27001:2013** A.6.1.1, A.7.2.1, A.7.2.2., A.8.2. 1, A.8.2.2, A.8.2.3,A.8.3.1, A.8.3.2, A.8.3.3, A.9.1.1, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5, A.10.1.1, A.11.1.4, A.11.1.5, A.11.2.1, A.11.2.5, A.11.2.7, A.11.2.9, A.13.1.1, A.13.1.3, A.13.2.1, A.13.2.3, A.13.2.4, A.14.1.2, A.14.1.3	Session layer encryption and secure protocols (e.g. Secure Sockets Layer (SSL)), for sensitive and regulated data in transit is protected/encrypted at the web, mobile, etc. application level (production and non-production) per NIST best practices/guidance; to include personally identifiable information (PII) shared by user (form/field based entry). Sensitive and regulated data at rest (production and non-production) is protected by native or 3rd party encryption technologies.	-3== No implementation of secure protocols or encryption technology (application or data repositories) -2== Inaccurate or lesser standard encryption/secure protocols per data type (e.g., financial, govt., etc.) -1== Deployment of archaic/legacy secure protocols
SE5	*All*	Whether the application/product has critical or high vulnerabilities (security assessments) that could potentially lead to exposed or leaked sensitive information and defined remediation plan(s)	=	Art.32	🚫	Not Included	Data Controller Questionnaire; Summary results from Pre-Certifications mentioned in Column H.	Security Expert	**NIST Cybersecurity Framework (CSF)** Identify: ID.SC-4. Respond: RS.AN -5/ **NIST SP 800-53 Rev. 5**/IR.A-5, SI-5, PM-15/ **HITRUST** Control Category 03.b, 08.d, 11.a, 13.q, 13.u/ **PCI DSS Requirement** 5, 6/ **FFIEC** Domain 3 Cybersecurity Controls: Secure Coding, Threat and Vulnerability Detection/ **ISO 27001:2013** A.15.2.1, A.15.2.2	Conduct initial and, at minimum, annual ongoing security assessments to include, where appropriate, but not limited to Static Application Security Testing (SAST)/Dynamic Application Security Testing (DAST), Penetration Testing, and continuous vulnerability management monitoring/scanning	-3== No testing/validation completed in the lifecycle of product development -2== No testing/validation completed in > 18 months -1== Lack of documented remediation/risk-based acceptance of identified High or Critical vulnerabilities
SE6	*All*	Whether data controller encrypts all Personally Identifiable Information at rest and in transport with the most respectful encrypted string and doesn't create a new persistent ID.	↑	Art.32(1)	🚫	Not Included	Data Controller Questionnaire	Security Expert	Data controller encrypts data at rest and in transport using optimal recommended methods for each type of info. Data controller doesn't create a new persistent ID.	Data controller encrypts data at rest and in transport using optimal recommended methods for each type of info. Data controller doesn't create a new persistent ID.	-3== No encryption in place on sensitive/regulated data (personally identifiable information) at any/all levels of the tech stack (e.g., data at rest, data in motion, etc.) -2== Lesser data standards and security/protection protocols (e.g., obfuscation/masking) used in lieu of encryption -1== Utilization of native encryption protocols vs. enhanced 3rd party encryption protocols and standards

3 - SAFE & RESPECTFUL COMMITMENT TESTS - TEMPLATE

TEST #	Me2B COMMITMENT	SAFE & RESPECTFUL COMMITMENT ATTRIBUTE	WHAT'S BEING MEASURED	GDPR MAP		NOTES &/OR DIFFERENCES BETWEEN GDPR & ISL	CPRA MAP		CPRA NOTABLE DIFFERENCES WITH CCPA	NOTES &/OR DIFFERENCES BETWEEN CPRA & ISL	PASSING BEHAVIORS (SCORE = 0)	FAILING BEHAVIORS (SCORES -1 to -3)
Test Scope: These tests should be run (duplicated) for each Me2B Commitment that exists in the chosed audit scope (i.e. webpages or UX flows in an app).												
ATTRIBUTE 1: CLEAR DATA PROCESSING NOTICE												
A1-1	*<xxx> Commitment*	*(1) Clear Data Processing Notice - Existence*	If there is a data processing notice available to the user.	=	Art.12(1); Recital 39(2); Recital 60(1)	In alignment	=	1798.130(5); 1798.100(a)	Adds that notice should be "prominently" displayed in privacy policy. Adds notice requirement for "shared" data. Adds stronger language to reinforce that Biz that "control the collection of" PI must provide notice.	In alignment	There is a data processing notice available.	-3 == Data processing notice is missing
A1-2	*<xxx> Commitment*	*(1) Clear Data Processing Notice - Understandability - Accessible*	If the data processing notice is present/available on the same screen as the commitment.	=	Art.12(1); Recital 39(4)	In alignment	=	Not Included See 1798.100(a); 1798.135(a); 1798.140(p); 999.301(l); 999.301(m); 999.301(p); 999.304; 999.305 for further analysis.	AG Regs add that notice should be designed & presented in a way that is easy to read & understandable in a format that draws the consumers attention.	In alignment	The data processing notice/information is available on the same screen as the commitment--without having to go to another page.	-2 == Data processing notice is not on the same screen.
A1-3	*<xxx> Commitment*	*(1) Clear Data Processing Notice - Understandability - Scope*	If the data processing notice explains (breaks out) data processing for each level of Me2B Commitment. E.g. the notice explains which information is collected for each type of commitment.	↑	Similar to Art. 13(1); Art. 13(2); Art. 14	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.	↑	Not Included See 1798.130(5) for further analysis.	Adds notice requirement of lists/ categories of PI.	B-s are legally required to provide notices that break out data processing into specific categories of PI & purposes that are very broad.	The data processing notice is either specific to the commitment, or, if general for the whole website/app, contains sections for each commitment level.	-3 == Data processing notice does not clarify data processing per Me2B Commitment.
A1-4	*<xxx> Commitment*	*(1) Clear Data Processing Notice - Understandability - Accessible*	If the data processing notice is accessible by assistive services.	=	Art. 12(7); Art. 21(5); Recital 60(5); Recital 60(6)	In alignment	=	999.305(a)(2)(c) and 999.305(a)(2)(d)	Maps to the AG Regs that are already in effect.	B-s are legally required to provide notice that is accessible to Me-s with disabilities. Notices must also be available in all languages in which the B ordinarily conducts business.	The data processing notice/information is accessible and rendered by assistive services.	-3 == The assistive screen reader is unable to read any of the notice. -2 == The assistive screen reader is unable to read most of the notice. -1 == The assistive screen reader is unable to read part of the notice.
A1-5	*<xxx> Commitment*	*(1) Clear Data Processing Notice - Understandability - Complete*	If the data processing notice of the <commitment name> (Me2B Deal) that the data subject receives on the website is complete, providing details: (1) the Me2B Deal Terms (quid pro quo) including subsidization and data monetization; (2) list of information collected (covering volunteered, observed and derived information); and (3) for each item of information, (a) legal basis for collection, (b) purpose for collecting the information including how it's used, (c) all data processors & co-controllers who receive it, and (d) how long the information is retained (by all data controllers and co-processors).	↑	Art. 13(1); Art. 13(2)	The Law allows the notice to be sufficient when recipients or "categories of recipients" are named. As such, our requirements are greater than what the law requires.	↑	Similar to 1798.100(a)(1) thru (a)(3).	Adds the majority of this language.	Our requirements are greater than what the law requires.	The information the data subject receives at the point of the commitment looks complete per cell 9E (i.e. includes all of the necessary categories/sections of information).	-3 == Processing notice is missing a section from the list in 9E.
A1-6	*<xxx> Commitment*	*(1) Clear Data Processing Notice - Understandability - Clear*	If the data processing notice of the <xxx> commitment is clear and easy to understand by the general population.	↑	Art. 7(2); Art. 4(11); Recital 42; Recital 39	No requirements that indicate a way to measure that the language is easy to understand. Otherwise, in alignment given that "by the general population" could be inferred from their broad language.	↑	Similar to 999.305(a)(2); 999.308(a)(2); 999.308(c); 999.315(h)(2)	Maps to the AG Regs that are already in effect.	In alignment 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 any reading comprehension test to determine the understandability of the notice.	The copy for the website notice for the <xxx> commitment is clear and easy to understand by the general population. Readable privacy policy for site is at grade level 6 or better (lower) as measured by: https://www.webfx.com/tools/read-able/flesch-kincaid.html https://datayze.com/readability-analyzer.php or other site.	-3 == Reading comprehension score is above Flesch Kincaid 8th grade level or similar readability score -1 == Reading comprehension score is above Flesch Kincaid 6th grade reading level or similar readability score
ATTRIBUTE 2: VIABLE PERMISSION												
A2-1	*<xxx> Commitment*	*(2A) Viable Permission - Understandability*	If the information the data subject receives at the point of the <xxx> commitment is sufficient to provide informed permission. (this is tested in Attribute 1--the rolled-up average scores for Attribute 1 satisfy this criteria.)	=	Art.4(11)	In alignment	↑	1798.140(H)	Adds "informed"	Mention of informed permission. Ties into understandability concepts in Attribute 1.	If the roll-up average scores for Attribute 1 is between 0 and -0.49.	If the roll-up average scores for Attribute 1 are =< -0.5
A2-2	*<xxx> Commitment*	*(2B) Viable Permission - Freely Given*	If the data subject freely gives permission for the <xxx> commitment.	=	Art.4(11); Recital 40	In alignment	=	1798.140(L); 1798.140(H)	Adds Definition of Dark Pattern & Consent.	In alignment	No dark patterns detected in the commitment UX.	Harmful patterns detected in <xxx> Commitment UX (range -1 to -3) Data subject is required to agree to terms of service prior to account creation. (-3)
A2-3	*<xxx> Commitment*	*(2C) Viable Permission - Intentional Action*	If the data subject performs an intentional action to enter the <xxx> commitment.	=	Art.4(11); Art.6(1); Art.7(1); Recital 42(1); Recital 42(3); Recital 43	In alignment	⃠	Similar to 1798.140(S); 1798.140(H)	Adds Definition of "Intentionally Interacts" & Consent	Under the CPRA, it's unclear if contracts of adhesion will or will not constitute an intentional action.	There is a discrete, permission UX for the commitment.	No consent or permission mechanism for the commitment. (-3)
A2-4	*<xxx> Commitment*	*(2D) Viable Permission - Flow to data processors*	If the data subject's permissions for data related to this commitment are passed to all third parties - co-data controllers and data processors.	=	Art.82(2); Art.28(1); Art. 28; Art.31; Recital 81	In alignment	=	999.314(c); 999.314(d); 999.314(e)	Maps to the AG Regs that are already in effect.	In alignment	Data controller confirms that data subject permissions for commitment are passed to all co-data controllers and data processors.	Permissions are not passed to co-data controllers or data processors (-3)
A2-5	*<xxx> Commitment*	*(2) Viable Permission - Appropriate Level of Control*	If 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.	↑	Recital 43(2); Recital 42(2)	Similar to the legal requirement that consent should be given for each purpose if the processing has multiple purposes. But our requirements go further by establishing an appropriate level of control for the commitment parameters.	⃠	Not Included.	Not Included	Not Included	Data subject has an appropriate level of control for the commitment parameters.	Data subject controls are are inadequate/insufficient/too coarse-grained. (-3) Data subject controls are somewhat inadequate/sub-optimal. (-1)
A2-6	*<xxx> Commitment*	*(2) Viable Permission - No Data Collection Before Permission Granted*	If the service collects commitment-related information before the data subject grants permission.	=	Art. 4; Recital 43(2); Recital 32	In alignment. GDPR requires a data subject to opt-in prior to collecting that data subject's personal data.	↑	Similar to 999.305(1); 999.305(5); 999.305(6)	Maps to the AG Regs that are already in effect.	The law is centered around notice at collection rather than granting of permission.	No commitment-related information is collected before the data subject grants permission.	Commitment-related information is collected before the data subject grants permission. (-3)
ATTRIBUTE 3: IDENTIFICATION MINIMIZATION												
A3-1	*<xxx> Commitment*	*(3) Identification Minimization - Data Controller*	Data subject identification comports to appropriate state of Me2B Lifecycle. Is the data subject "jonkey" being used to correlate behavioral data in an expected way by the data controller? Is the data subject being actively tracked beyond the expected scope of this commitment per the Me2B Lifecycle?	↑	Art.5(1)(e)	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."	⃠	Not Included	Not Included	Not Included	Identification and data subject profiling performed by the data controller comports with the Me2B approved identification for the commitment.	Identification performed exceeds the Me2B-approved identification for the commitment (refer to Figure 4 in the Me2B Safe Specification Introduction). (-3)
A3-2	*<xxx> Commitment*	*(3) Identification Minimization - Data Processors and Co-Controllers*	Data subject identification comports to appropriate state of Me2B Lifecycle. Is the data subject "jonkey" being used to correlate behavioral data in an expected way by data processors & co-controllers? Is the data subject being actively tracked beyond the expected scope of this commitment per the Me2B Lifecycle? Note: testing the Local Storage Commitment covers advertising and analytics related cookies or other jonkeys.	⃠	Not Included	Not Included	⃠	Not Included	Not Included	Not Included	Identification and data subject profiling performed by data processors and co-controllers comports with the Me2B approved identification for the commitment.	Identification performed exceeds the Me2B-approved identification for the commitment (refer to Figure 4 in the Me2B Safe Specification Introduction). (-3) Service is using shared jonkeys with advertisers/analytics/data brokers outside of the expected Me2B Deal. (-3)
ATTRIBUTE 4: DATA COLLECTION MINIMIZATION												
A4-1	*<xxx> Commitment*	*(4) Data Collection Minimization*	The minimum **volunteered** information required for this commitment is (refer to Figure 5 in the Me2B Safe Specification Introduction for Me2B-approved data for this commitment). No other data is required.	=	Art.5(1)(c); Art.25	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.	⃠	Not Included	Not Included	Not Included	Website only collects the information described in Figure 5 and no additional information when entering this commitment.	Other lower-harm/lower-sensitivity information also collected. (-1, -2) Harmful/sensitive information also collected. (-3)
A4-2	*<xxx> Commitment*	*(4) Data Collection Minimization*	The minimum **observed** information required for this commitment is (refer to Figure 5 in the Me2B Safe Specification Introduction for Me2B-approved data for this commitment).	⃠	Not Included	Not Included	⃠	Not Included but see 999.323(f); 999.306(d); 999.313(c)(3); 1798.140(c); 1798.100 (c)	AG Regs that are already in effect.	Regs make inferences about Data minimization. Stating that B-s are not obligated to provide or delete data if they maintain deidentified data.	Website only collects the information described in Figure 5 and no additional information when entering this commitment.	Other lower-harm/lower-sensitivity information also collected. (-1, -2) Harmful/sensitive information also collected. (-3)
A4-3	*<xxx> Commitment*	*(4) Data Collection Minimization*	The minimum **derived** information required for this commitment is (refer to Figure 5 in the Me2B Safe Specification Introduction for Me2B-approved data for this commitment).	⃠	Not Included	Not Included	⃠	Not Included	Not Included	Not Included	Website only collects the information described in Figure 5 and no additional information when entering this commitment.	Other lower-harm/lower-sensitivity information also collected. (-1, -2) Harmful/sensitive information also collected. (-3)
ATTRIBUTE 5: PRIVATE BY DEFAULT												
A5-1	*<xxx> Commitment*	*(5) Private by Default*	The individual doesn't have to modify any privacy settings in order for the data associated with this commitment to be used only in the context of this commitment and Me2B Deal.	↑	Art. 25(2)	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.	⃠	Not Included	Not Included	Not Included	Data associated with this commitment is not shared to unnecessary data processors by default.	There are settings that the data subject must configure in order to assure shared data in this commitment is used only this commitment's Me2B Deal. (-3)
ATTRIBUTE 6: REASONABLE DATA USE & SHARING BEHAVIOR												

3 - SAFE & RESPECTFUL COMMITMENT TESTS - TEMPLATE

TEST #	Me2B COMMITMENT	SAFE & RESPECTFUL COMMITMENT ATTRIBUTE	WHAT'S BEING MEASURED		GDPR MAP	NOTES &/OR DIFFERENCES BETWEEN GDPR & ISL		CPRA MAP	CPRA NOTABLE DIFFERENCES WITH CCPA	NOTES &/OR DIFFERENCES BETWEEN CPRA & ISL	PASSING BEHAVIORS (SCORE = 0)	FAILING BEHAVIORS (SCORES -1 to -3)
A6-1	<xxx> *Commitment*	*(6) Reasonable Data Use Behavior*	If the information use claims provided by the data controller match the observed data use [by the data controller].	⊘	Art. 6; Art. 24(1)	Not included, but a strong argument could be made that these controls could be inferred from the law. For lawful processing, the data may only be collected under viable legal basis. (Art. 6 Lawfulness of Processing)	⊘	Not included.	Not Included	Not Included	Observed data controller data *use* matches supporting information provided by data controller in the questionnaire.	-3 == Observed data *use* behavior for the commitment differs from information in the data controller provided questionnaire responses.
A6-2	<xxx> *Commitment*	*(6) Reasonable Data Use Behavior*	If the information use by the data controller is appropriate to the commitment.	⊘	Art. 6; Art. 24(1)	Not included, but a strong argument could be made that these controls could be inferred from the law.	⊘	Not included, but similar to 1798.100(c);1798.140(e)	Adds applicable language	Legally the information used by B-s need to 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.	Service only uses <xxx> commitment information in order to provide <commitment name> services, as defined by the Me2B deal terms for the commitment.	-3 == Data controller uses data collected for this commitment outside of the bounds of the agreed-upon Me2B deal terms for this commitment, in a way that exposes the data subject to serious risks. -2 == Data controller uses data collected for this commitment outside of the bounds of the agreed-upon Me2B deal terms for this commitment in a way that exposes the data subject to moderate risks. -1 == Data controller uses data collected for this commitment outside of the bounds of the agreed-upon Me2B deal terms for this commitment in a way that exposes the data subject to low risks.
A6-3	<xxx> *Commitment*	*(6) Reasonable Data Sharing Behavior*	If the information sharing claims provided by the data controller match the observed data sharing [by the data controller].	⊘	Art. 6; Art. 24(1)	Not included, but a strong argument could be made that these controls could be inferred from the law.	↑	1798.100(a)(1)	Adds "incompatible w/ disclosed purpose for which PI was collected"	Legal violation arises if a B collects additional categories of PI w/o providing notice or uses PI collected for additional purposes incompatible w/ disclosed purpose.	Observed data controller data *sharing* matches supporting information provided by data controller in the questionnaire.	-3 == Observed data *sharing* behavior for the commitment differs from information in the data controller provided questionnaire responses.
A6-4	<xxx> *Commitment*	*(6) Reasonable Data Sharing Behavior*	If the information sharing [by the data controller] with data processors and co-controllers is appropriate to the commitment.	↑	Art. 28; Art. 29; Art. 31; Recital 81	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.	↑	Not included, but similar to 1798.100(d); 1798.140(e); 1798.140(ag); 999.314(c)	Adds most of the applicable language	B has a legal limitation to share PI for limited specified purposes. Co-controller's are prohibited from using info for any purpose other than purpose specified.	Service only shares <xxx> commitment information with mandatory data processors in order to provide <commitment name> services.	-3 == Service shares <xxx> commitment information with advertisers, OR with any data processor using a globally unique joinkey. -2 == Service shares <xxx> commitment information with analytics platforms without a globally unique joinkey -1 == Service shares <xxx> commitment information with other 3rd parties.
A6-5	<xxx> *Commitment*	*(6) Reasonable Data Use & Sharing Behavior*	If the information use & sharing is comparable to the industry norm.	⊘	Not Included	Not Included	⊘	Not Included	Not Included	Not Included	Number of data processors in the service is within 10% of industry average.	-1 == # data processors in the service is >11% and < 35% of industry average; -2 == # data processors in the service is > 36% and < 50% of industry average; -3 == # data processors in service is > 51% of industry average.
ATTRIBUTE 7: DATA PROCESSING MATCHES DATA SUBJECT'S PREFERENCES & PERMISSIONS												
A7-1	<xxx> *Commitment*	*(7) Data Processing Matches data subject's Preferences & Permissions*	If the observed *data collection* matches the data subject's permissions and preferences.	⊜	Art. 4(11); Art. 6; Art. 7; Recital 42; Recital 43	While these details are not expressly mentioned in the law, for data controllers to lawfully process data they must have the data subject's consent (or another legal bases) meaning that they must comport with their permissions & preferences in theory.	⊘	Not Included	Not Included	Not Included	If the UX offers permission options in the <xxx> Commitment, changes pertaining to data collection are accurately reflected as soon as the data subject makes any changes.	For multiple options in the commitment: -3 == none of the options change the service's behavior in the expected way, -2 == 50% of the options change the service's behavior in the expected way, -1 == 20% of the options change the service's behavior in the expected way.
A7-2	<xxx> *Commitment*	*(7) Data Processing Matches data subject's Preferences & Permissions*	If the observed data controller *data use and sharing* matches the data subject's permissions and preferences.	⊘	Art. 4(11); Art. 6; Art. 7; Recital 42; Recital 43		⊘	Not Included See 1798.100(a)(c); 1798.145(i)(2)	Adds applicable language	Legal violation arises if a B shares PI w/o providing notice or shares Me's collected PI after Me opted out.	If the UX offers permission options in the <xxx> Commitment, changes pertaining to data controller data use and sharing are accurately reflected as soon as the data subject makes any changes.	For multiple options in the commitment: -3 == none of the options change the data controller's behavior in the expected way, -2 == 50% of the options change the data controller's behavior in the expected way, -1 == 20% of the options change the data controller's behavior in the expected way.
A7-3	<xxx> *Commitment*	*(7) Data Processing Matches data subject's Preferences & Permissions*	If the observed data processor and co-data controller data use and sharing matches the data subject's permissions and preferences.	⊘	Art. 4(11); Art. 6; Art. 7; Recital 42; Recital 43		⊘	Not Included	Not Included	Not Included	If the UX offers permission options in the <xxx> Commitment, changes pertaining to data processor & co-controller data use and sharing are accurately reflected as soon as the data subject makes any changes.	For multiple options in the commitment: -3 == none of the options change the data processors'/co-controllers' behavior in the expected way, -2 == 50% of the options change the data processors'/co-controllers'behavior in the expected way, -1 == 20% of the options change the data processors'/co-controllers'behavior in the expected way.
ATTRIBUTE 8: DATA PROCESSING MATCHES POLICIES												
A8-1	<xxx> *Commitment*	*(8) Data Processing Matches Policies*	That the observed data collection matches what's described in the Privacy Policy as collected in the Policy Raw Data	⊜	Art.6(1); Art. 7; Art.13(1); Art. 14; Recital 42; Recital 43	The law does not go into this detail but there is a strong argument that this could be inferred.	⊜	(999.305(6); 1798.130(5); 1798.100(a)	Adds B-s that "control the collection of" PI must provide notice.	Law does not explicitly state that the observed data match the policy but it can easily be inferred from their rule language.	Observed behavior mostly matches privacy policy.	-3 == Observed data collection behavior mostly doesn't match the privacy policy in substantial ways. -2 == Observed data collection behavior has one or more serious mismatch with the privacy policy. -1 == Observed data collection behavior has one or more less serious mismatches with the privacy policy.
A8-2	<xxx> *Commitment*	*(8) Data Processing Matches Policies*	That the observed data collection matches what's described in the Terms of Service as collected in the Policy Raw Data	⊘	Art.6(1); Art. 7; Art.13(1); Art. 14; Recital 42; Recital 43	The law does not go into this detail but there is a strong argument that this could be inferred.	⊘	1798.130(5)	No major changes	No direct mention of TOS in the law it is just referred to as other policies.	Observed behavior mostly matches the Terms of Service.	-3 == Observed data collection behavior mostly doesn't match the terms of service in substantial ways. -2 == Observed data collection behavior has one or more serious mismatch with the terms of service. -1 == Observed data collection behavior has one or more less serious mismatches with the terms of service.
A8-3	<xxx> *Commitment*	*(8) Data Processing Matches Policies*	That the observed data use behavior of the data controller matches what's described in the Privacy Policy as collected in the Policy Raw Data	⊘	Art.6(1); Art. 7; Art.13(1); Art. 14; Recital 42; Recital 43	The law does not go into this detail but there is a strong argument that this could be inferred.	⊘	Not Included	Not Included	Not Included	Observed behavior mostly matches privacy policy.	-3 == Observed data controller data use behavior mostly doesn't match the privacy policy in substantial ways -2 == Observed data controller data use behavior has one or more serious mismatch with the privacy policy. -1 == Observed data controller data use behavior has one or more less serious mismatches with the privacy policy.
A8-4	<xxx> *Commitment*	*(8) Data Processing Matches Policies*	That the observed data use behavior of the data controller matches what's described in the Terms of Service as collected in the Policy Raw Data	⊘	Art.6(1); Art. 7; Art.13(1); Art. 14; Recital 42; Recital 43	The law does not go into this detail but there is a strong argument that this could be inferred.	⊘	Not Included	Not Included	Not Included	Observed behavior mostly matches Terms of Service.	-3 == Observed data controller data use behavior mostly doesn't match the terms of service in substantial ways -2 == Observed data controller data use behavior has one or more serious mismatch with the terms of service. -1 == Observed data controller data use behavior has one or more less serious mismatches with the terms of service.
A8-5	<xxx> *Commitment*	*(8) Data Processing Matches Policies*	That the observed data sharing behavior of the data controller matches what's described in the Privacy Policy as collected in the Policy Raw Data	⊘	Not Included	Not Included	⊘	Not Included	Not Included	Not Included	Observed data controller data sharing behavior mostly matches privacy policy; and no data processors or co-data controllers are observed that ARENT included in the privacy policy.	-3 == Observed data controller data sharing behavior mostly doesn't match the privacy policy in substantial ways, and shares data with data processors or co-data controllers who aren't included in the privacy policy -2 == Observed data controller data sharing behavior has one or more serious mismatch with the privacy policy. -1 == Observed data controller data sharing behavior has one or more less serious mismatches with the privacy policy.
A8-6	<xxx> *Commitment*	*(8) Data Processing Matches Policies*	That the observed data sharing behavior of the data controller matches what's described in the Terms of Service as collected in the Policy Raw Data	⊘	Not Included	Not Included	⊘	Not Included	Not Included	Not Included	Observed data controller data sharing behavior mostly matches terms of service; and no data processors or co-data controllers are observed that ARENT included in the terms of service.	-3 == Observed data controller data sharing behavior mostly doesn't match the terms of service in substantial ways, and shares data with data processors or co-data controllers who aren't included in the terms of service. -2 == Observed data controller data sharing behavior has one or more serious mismatch with the terms of service. -1 == Observed data controller data sharing behavior has one or more less serious mismatches with the terms of service.
ATTRIBUTE 9: REASONABLE COMMITMENT DURATION												
A9-1	<xxx> *Commitment*	*(9) Reasonable Commitment Duration*	If the default commitment duration is reasonable & appropriate for the commitment and the type of service. For ongoing-long-lived commitments: The <xxx> Commitment is expected to end when either the data subject unenrolls from it, or the data controller discontinues the service (or ends the commitment per the Terms of Service).	↑	Art.5(e); Recital 39(10)	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.	↑	Similar to 1798.100(a)(3)	Added language regarding the length of retention	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.	The default commitment duration matches the Me2B approved duration for the commitment.	The default duration for the commitment exceeds the Me2B Approved duration for the commitment (-3): COMMITMENT <--> Me2B APPROVED 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 Commitment Until data subject or data controller terminates
ATTRIBUTE 10: COMMITMENT TERMINATION & CHANGE BEHAVIOR												
A10-1	<xxx> *Commitment*	*(10A) Commitment Termination & Change Behavior - Easy to End/Change Commitment*	If it's easy to stop or change the commitment.	⊘	Art. 21; Art.18	No, but the GDPR does provide Data Subjects with the right to object to data processing at any time.	⊘	Not Included	Not Included	Not Included	Easy to stop or change <xxx> commitment.	-3 == No way to change/end <xxx> commitment; -2 == Difficult to find and change/end <xxx> commitment; -1 == Difficult to find OR change/end <xxx> commitment.
A10-2	<xxx> *Commitment*	*(10B) Commitment Termination & Change Behavior - Record*	If the data subject receives or has access to a record of requested changes.	⊘	Art. 12(3)(1)	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.	↑	Similar to 999.313(a); 999.313(d)(4); 999.314(d)(5); 999.316(b); 999.316(c)	Maps to the AG Regs that are already in effect.	A record for termination is only legally required for request to delete and request to know. A record of all commitments is not legally required.	Data subject can view online or separately receives a confirmation of changes.	Data subject neither has a way to view online NOR receives a separate confirmation of changes. (-3)
A10-3	<xxx> *Commitment*	*(10C) Commitment Termination & Change Behavior - Data Removal*	If the data controller removes or changes commitment-related data upon request.	=	Art. 17; Art. 19; Recital 39(11); Recital 65; Recital 66	In alignment.	↑	1798.105(a);1798.105(c)(1) & (c)(3); 999.313(d)(2); 999.313(8); 999.314(e); See 1798.105(d) for exceptions	Added significant additional language	The law only requires B-s to remove or change data upon a Me's request to delete information…some exceptions do apply.	Data controller removes all data relating to the commitment.	Data controller retains personally identified information relating to the <xxx> commitment. (-3)
A10-4	<xxx> *Commitment*	*(10D) Commitment Termination & Change Behavior - Permissions Flow to data processors*	If all co-data controllers and data processors receive notification and change/delete data upon commitment end/change.	=	Art. 19; Art. 18(2); Art. 28(3)(g); Art. 31; Recital 81	In alignment, all data controllers must delete Data Subject's personal data and notify co-controllers.	↑	1798.105(c)(1) & (c)(3)	Added the effective language	For requests to delete the law requires notification to all service providers, contractors and third parties.	All co-data controllers and data processors receive notification and delete data upon commitment end/change.	Co-data controllers and data processors do not receive notification of commitment change/termination and do not delete data. (-3) Co-data controllers and data processors do receive notification but don't delete data on commitment termination. (-3)

4 - LOCATION COMMITMENT REQUIREMENTS

TEST #	Me2B COMMITMENT	SAFE & RESPECTFUL COMMITMENT ATTRIBUTE	WHAT'S BEING MEASURED	GDPR MAP		CCPA/CPRA MAP		DATA USED TO MEASURE	EXPERTISE NEEDED TO EVALUATE	BEST PRACTICE (SCORE = +1)	PASSING BEHAVIORS (SCORE = 0)	FAILING BEHAVIORS (SCORES -1 to -3)
LC1	*Location Commitment - Browser Level*	*All*	If the website uses browser level location tracking & consent	↑	B-s may collect location data only after receiving Me's consent.	↑	1798.140(w); Precise geolocation is treated as "Sensitive PII". Me-s have right to limit use to what is necessary to perform the services or provide the goods reasonably expected by an average consumer.	Observed UX	UX Expert	No use of browser level location tracking & consent.	No use of browser level location tracking & consent.	Use of browser level tracking & location consent. (-3)
LC2	*Location Commitment - data controller Level*	*(5) Private by Default*	If the site automatically determines location without data subject permission.	=	Art.6 violation. Not a lawful processing of personal data.	🚫	Not Included	Observed UX	UX Expert	Site does not automatically calculate location, and asks for consent to use location information. NA?	Site does not automatically calculate location, and asks for consent to use location information.	Site automatically calculates location without asking for permission (-3).

5 - ACCOUNT CREATION COMMITMENT REQUIREMENTS

TEST #	Me2B COMMITMENT	WHAT'S BEING MEASURED		GDPR MAP		CCPA/CPRA MAP	DATA USED TO MEASURE	RTISE NEEDED TO EVALU	BEST PRACTICE (SCORE = +1)	PASSING BEHAVIORS (SCORE = 0)	FAILING BEHAVIORS (SCORES -1 to -3)
SCENARIO: ACCOUNT CREATION											
MM1	*Account Creation Commitment*	Plain text fields in password/pin creation	🚫	Not Included	🚫	Not Included	Observed UX	UX Expert	Not collected as plain text.	Not collected as plain text.	Collected as plain text (-3).
MM2	*Account Creation Commitment*	Plain text fields in password security questions	🚫	Not Included	🚫	Not Included	Observed UX	UX Expert	Not collected as plain text.	Not collected as plain text.	Collected as plain text (-3).
SCENARIO: USER LOGGED IN - "REMEMBER ME" OPTION											
MM3	*Account Creation Commitment*	"Remember Me" option presented to data subject.	🚫	Not Included	🚫	Not Included	Observed UX	UX Expert	Option only presented for high-frequency interaction relationships, and only for low-risk transactions.	Option only presented for high-frequency interaction relationships, and only for low-risk transactions.	Option presented for low-frequency interaction relationships, and for high-risk transactions. (-3)
MM4	*Account Creation Commitment*	"Remember Me" enabling.	🚫	Not Included	🚫	Not Included	Observed UX	UX Expert	Easy to understand exactly what gets remembered and for how long; shouldn't be too easy to turn on; Defaults to disabled.	Easy to understand exactly what gets remembered and for how long; shouldn't be too easy to turn on; Defaults to disabled.	Defaults to enabled. (-3) Harmful patterns manipulating data subject to turn on Remember Me. (-2)
MM5	*Account Creation Commitment*	"Remember Me" disabling.	🚫	GDPR has the same overarching policy value as CCPA/CPRA	🚫	Not expressly mentioned but the law does have an overarching policy value of making things easy to read & understand. See 1798.185 (a)(20)(C)(iii) and 999.305	Observed UX	UX Expert	Easy to find and disable "Remember Me"	Easy to find and disable "Remember Me"	-3 == No way to disable Remember Me, -2 == Hard to find and disable Remember Me, -1 == Hard to find or disable Remember Me.
SCENARIO: USER HAS ACCOUNT BUT NOT LOGGED IN, N											
MM6	*Account Creation Commitment*	Validates that no personal information is displayed when not logged in and "not remembered"	🚫	Not Included	🚫	Not Included	Observed UX	UX Expert	Website behaves exactly as in the "Local Storage consent" state, before an account was created.	Website behaves exactly as in the "Local Storage consent" state, before an account was created.	Website continues to remember, recognize and personally respond to data subject (-3).
SCENARIO: USER HAS ACCOUNT, IS LOGGED IN & REMEM											
MM7	*Account Creation Commitment*	If too sensitive information is displayed/exposed when "remembered".	🚫	Not Included	🚫	Not Included	Observed UX	UX Expert	Website doesn't allow for extremely sensitive personal information to be displayed or exposed on the device.	Website doesn't allow for extremely sensitive personal information to be displayed or exposed on the device.	Website displays extremely sensitive personal infromation on the device without being logged in. (-3)