<table>
<thead>
<tr>
<th>VERSION</th>
<th>DATE</th>
<th>PLATFORMS</th>
<th>EDITORS</th>
<th>CONTRIBUTORS</th>
<th>DESCRIPTION OF CHANGES</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.1</td>
<td>08/21/21</td>
<td>Websites</td>
<td>L. LeVasseur</td>
<td>RTS WG</td>
<td>Candidate Working Group Approval draft</td>
</tr>
<tr>
<td>0.2</td>
<td>10/10/21</td>
<td>Websites</td>
<td>L. LeVasseur</td>
<td>RTS WG</td>
<td>WG Approved Draft</td>
</tr>
<tr>
<td>0.7</td>
<td>12/28/21</td>
<td>Websites, Mobile Apps</td>
<td>L. LeVasseur</td>
<td>RTS WG</td>
<td>Simplified after lack of comments in two review periods.</td>
</tr>
<tr>
<td>1.0</td>
<td>04/26/22</td>
<td>Websites, Mobile Apps</td>
<td>L. LeVasseur</td>
<td>RTS WG</td>
<td>Publication version.</td>
</tr>
<tr>
<td>1.05</td>
<td>04/30/22</td>
<td>Websites, Mobile Apps</td>
<td>L. LeVasseur, Daniella Doem</td>
<td>L. LeVasseur, Daniella Doem</td>
<td>Added CPRA and GDPR Mapping</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Changed name of Me2B Marriage Commitment commitment; and organization name.</td>
</tr>
<tr>
<td>1.06</td>
<td>06/06/22</td>
<td>Websites, Mobile Apps</td>
<td>L. LeVasseur</td>
<td>L. LeVasseur, Daniella Doem</td>
<td>Publication version.</td>
</tr>
<tr>
<td>1.1</td>
<td>07/05/22</td>
<td>Websites, Mobile Apps</td>
<td>L. LeVasseur, Daniella Doem</td>
<td>L. LeVasseur, Daniella Doem</td>
<td>Publication version.</td>
</tr>
</tbody>
</table>
This workbook constitutes the ISL Safe SW Specification Core Requirements for Websites and Mobile Apps.

Sheet 1: Title Page
Sheet 2: Revision History
Sheet 3: Table of Contents
Sheet 4: Contributors
Sheet 5: 1 - Audit Introduction
Sheet 6: 2 - Requirements for All Commitments
Sheet 7: 3 - Per Commitment Requirements
Sheet 8: 4 - Location Commitment Specific Tests
Sheet 9: 5 - Account Creation Commitment Specific Tests
CONTRIBUTORS

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

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

<table>
<thead>
<tr>
<th>Test Scope</th>
<th>These tests apply to the overall service and are independent of the Me2B commitments that appear in the service.</th>
<th>Test</th>
<th>Make Commitment</th>
<th>What's Being Measured</th>
<th>USEP MAP</th>
<th>ODDA MAP</th>
<th>DATA USED TO MEASURE</th>
<th>EXPERTISE NEEDED TO EVALUATE</th>
<th>BEST PRACTICE (SCORE = +1)</th>
<th>PASSING BEHAVIOR (SCORE = -1)</th>
<th>FAILING BEHAVIOR (SCORE = -1.5 – -3)</th>
</tr>
</thead>
<tbody>
<tr>
<td>AL1</td>
<td>AL1</td>
<td>Data controller use the OECD’s transparency and consent framework (ART 7)?</td>
<td>Yes Included</td>
<td>Yes Included</td>
<td>Data Controller Questionnaire</td>
<td>One supply report</td>
<td>NA</td>
<td>Do not use the OECD’s ART 7. Did not show presenting an opt-out choice, and every time on an ART 7 is a violation of the ART 7.</td>
<td>AL1</td>
<td>AL1</td>
<td>AL1</td>
</tr>
<tr>
<td>AL2</td>
<td>AL1</td>
<td>Data controller use the GDPR’s transparency and consent framework (ART 13)?</td>
<td>Yes Included</td>
<td>Yes Included</td>
<td>Data Controller Questionnaire</td>
<td>One supply report</td>
<td>NA</td>
<td>Do not use the GDPRs ART 13. Did not make clear that the data processor support opting out. Options need to be clearly showing ENS</td>
<td>AL2</td>
<td>AL2</td>
<td>AL2</td>
</tr>
<tr>
<td>AL3</td>
<td>AL2</td>
<td>Data controller use the Native Knowledge sharing with information with data brokers.</td>
<td>Yes, Yes; See Additional, 776.0</td>
<td>Yes, Yes; See Additional, 776.0</td>
<td>Data Controller Questionnaire</td>
<td>One supply report</td>
<td>NA</td>
<td>Do not use the data broker added to sharing noninvasive data.</td>
<td>AL3</td>
<td>AL3</td>
<td>AL3</td>
</tr>
<tr>
<td>AL4</td>
<td>AL3</td>
<td>Whether data subject can request changes in Personal Data</td>
<td>Yes, Yes; Yes, Yes</td>
<td>Yes, Yes; Yes, Yes</td>
<td>Data Controller Questionnaire</td>
<td>One supply report</td>
<td>NA</td>
<td>Do not use of data brokers.</td>
<td>AL4</td>
<td>AL4</td>
<td>AL4</td>
</tr>
<tr>
<td>AL5</td>
<td>AL4</td>
<td>Whether data subject can request changes in Personal Data</td>
<td>Yes, Yes; Yes, Yes</td>
<td>Yes, Yes; Yes, Yes</td>
<td>Data Controller Questionnaire</td>
<td>One supply report</td>
<td>NA</td>
<td>Do not use of data brokers.</td>
<td>AL5</td>
<td>AL5</td>
<td>AL5</td>
</tr>
<tr>
<td>AL6</td>
<td>AL5</td>
<td>Whether the privacy policy is for the actual data controller?</td>
<td>Not Included</td>
<td>Not Included</td>
<td>Privacy Policy</td>
<td>NA</td>
<td>Do not use of data brokers.</td>
<td>AL6</td>
<td>AL6</td>
<td>AL6</td>
<td>AL6</td>
</tr>
<tr>
<td>AL7</td>
<td>AL6</td>
<td>Whether the privacy policy is for the actual data controller?</td>
<td>Not Included</td>
<td>Not Included</td>
<td>Privacy Policy</td>
<td>NA</td>
<td>Do not use of data brokers.</td>
<td>AL7</td>
<td>AL7</td>
<td>AL7</td>
<td>AL7</td>
</tr>
<tr>
<td>AL8</td>
<td>AL7</td>
<td>Whether the terms of service policy is for the actual data controller?</td>
<td>Not Included</td>
<td>Not Included</td>
<td>Terms of service Policy</td>
<td>NA</td>
<td>Do not use of data brokers.</td>
<td>AL8</td>
<td>AL8</td>
<td>AL8</td>
<td>AL8</td>
</tr>
<tr>
<td>AL9</td>
<td>AL8</td>
<td>Whether encryption standards/protocols are employed as data and network security to prevent unauthorized access to data or data repositories</td>
<td>Not Included</td>
<td>Not Included</td>
<td>Data supply expert</td>
<td>NA</td>
<td>Do not use of data brokers.</td>
<td>AL9</td>
<td>AL9</td>
<td>AL9</td>
<td>AL9</td>
</tr>
<tr>
<td>AL10</td>
<td>AL9</td>
<td>Whether data controller doesn’t create a new persistent ID.</td>
<td>Not Included</td>
<td>Not Included</td>
<td>Terms of Service Policy</td>
<td>NA</td>
<td>Do not use of data brokers.</td>
<td>AL10</td>
<td>AL10</td>
<td>AL10</td>
<td>AL10</td>
</tr>
</tbody>
</table>

**NOTES:**
- **Security and Technical Capability to Protect:**
  - 1 = no on-site security and technical capability to protect sensitive or regulated data.
  - 2 = on-site security and technical capability to protect sensitive or regulated data,
  - 3 = on-site security and technical capability to protect sensitive or regulated data, 
  - 4 = on-site security and technical capability to protect sensitive or regulated data, 
  - 5 = on-site security and technical capability to protect sensitive or regulated data, 
  - 6 = on-site security and technical capability to protect sensitive or regulated data, 
  - 7 = on-site security and technical capability to protect sensitive or regulated data, 
  - 8 = on-site security and technical capability to protect sensitive or regulated data, 
  - 9 = on-site security and technical capability to protect sensitive or regulated data, 
  - 10 = on-site security and technical capability to protect sensitive or regulated data, 

- **Best Practice (SCORE = +1):**
  - Options that indicate world-class, best-in-class security and technical capability to protect sensitive or regulated data.

- **Passing Behavior (SCORE = -1):**
  - Options that indicate minimal security and technical capability to protect sensitive or regulated data.

- **Failing Behavior (SCORE = -1.5):**
  - Options that indicate poor security and technical capability to protect sensitive or regulated data.
### 3. SAFE & RESPECTFUL COMMITMENT TESTS - TEMPLATE

<table>
<thead>
<tr>
<th>ATTRIBUTE</th>
<th>WHAT'S BEING MEASURED</th>
<th>PASSING BEHAVIORS (SCORE = 0)</th>
<th>FAILING BEHAVIORS (SCORE = -3)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 - Clear Data Processing Notice</td>
<td>Understandability</td>
<td>-3 == Processing notice is missing a section from the list in 9E.</td>
<td>-3 == Processing notice is missing a section from the list in 9E.</td>
</tr>
<tr>
<td>2 - Viable Permission</td>
<td>Understandability</td>
<td>-3 == Permissions are not passed to co-data controllers or processors.</td>
<td>-3 == Permissions are not passed to co-data controllers or processors.</td>
</tr>
<tr>
<td>3 - Data Collection Minimization</td>
<td>Understandability</td>
<td>-3 == Data collection is unreasonably extensive.</td>
<td>-3 == Data collection is unreasonably extensive.</td>
</tr>
</tbody>
</table>

**PASSING BEHAVIORS (SCORE = 0)**

- 1 Clear Data Processing Notice - Understandability
  - Data processing notice is available.
    - Art. 25(2)
    - Art. 28(1)
    - Art. 82(2)
    - Art. 4(11)
    - Art. 13(1)
    - Art. 13(2)
    - Art. 12(1)
    - Recital 39(2)
    - Recital 39(4)
    - Recital 42(1)
    - Recital 42(5)
    - Recital 43(2)
    - Recital 43(5)

- 2 Viable Permission - Understandability
  - Viable permission is understood.
    - Art. 21(5)
    - Art. 12(7)
    - Art. 4(11)
    - Art. 7(2)
    - Art. 4(11)
    - Art. 13(1)
    - Art. 13(2)

- 3 Data Collection Minimization
  - Data collection is limited.
    - Art. 21(5)
    - Art. 12(7)
    - Art. 4(11)
    - Art. 7(2)
    - Art. 4(11)
    - Art. 13(1)
    - Art. 13(2)

**FAILING BEHAVIORS (SCORE = -3)**

- 1 Clear Data Processing Notice - Understandability
  - Data processing notice is not available.
    - No consent or permission mechanism for the commitment.
      - Art. 25(2)
      - Art. 28(1)
      - Art. 82(2)
      - Art. 4(11)
      - Art. 13(1)
      - Art. 13(2)
      - Art. 12(1)
      - Recital 39(2)
      - Recital 39(4)
      - Recital 42(1)
      - Recital 42(5)
      - Recital 43(2)
      - Recital 43(5)

- 2 Viable Permission - Understandability
  - Viable permission is not understood.
    - No consent or permission mechanism for the commitment.
      - Art. 25(2)
      - Art. 28(1)
      - Art. 82(2)
      - Art. 4(11)
      - Art. 13(1)
      - Art. 13(2)
      - Art. 12(1)
      - Recital 39(2)
      - Recital 39(4)
      - Recital 42(1)
      - Recital 42(5)
      - Recital 43(2)
      - Recital 43(5)

- 3 Data Collection Minimization
  - Data collection is excessive.
    - Art. 21(5)
    - Art. 12(7)
    - Art. 4(11)
    - Art. 7(2)
    - Art. 4(11)
    - Art. 13(1)
    - Art. 13(2)

---

**Additional Notes**

- For each commitment, the data processing notice/information is available on the website. The data processing notice/information is easy to read & understandable in a format that draws the consumer's attention to the notice. Notice is explicitly required when the consumer is not already aware of required information.

- The data processing notice/information is available in a language that is comprehensive and suitable for the subject matter.

- The data processing notice/information is available in the language used by the consumer at the time of the determination of the means for the collection, use, or disclosure of personal data.
<table>
<thead>
<tr>
<th>ATTRIBUTE</th>
<th>COMMITMENT TERMINATION &amp; CHANGE BEHAVIOR</th>
</tr>
</thead>
<tbody>
<tr>
<td>10A</td>
<td>Commitment Termination &amp; Change Behavior</td>
</tr>
<tr>
<td>9</td>
<td>Reasonable Commitment Duration</td>
</tr>
<tr>
<td>8</td>
<td>Data Processing Matches Policies</td>
</tr>
</tbody>
</table>

- **Data Removal**
  - If the data subject receives or has access to a record of requested changes.
  - If the data subject removes all data relating to the commitment.

- **Record Change/Delete Data Upon Commitment End/Change.**
  - If the data subject makes any changes.
  - If the data subject removes all data relating to the commitment.

- **Commitment**
  - If the data subject removes all data relating to the commitment.

- **Commitment, changes pertaining to data processor & co-data controller.**
  - If the information sharing [by the data controller] with data processors or co-data controllers who aren't included in the terms of service.

- **Commitment, changes pertaining to data controller data use.**
  - If the observed data controller data use behavior mostly doesn't match the privacy policy in substantial ways.

- **Commitment, changes pertaining to data collection.**
  - If the observed data controller data processing behavior mostly doesn't match the privacy policy in substantial ways.

- **Commitment, changes pertaining to data collection & use for multiple options in the commitment.**
  - If the observed data controller data processing behavior mostly doesn't match the privacy policy in substantial ways.

### Table: Data Subjects' Commitments

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Score</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>10A</td>
<td>Commitment Termination &amp; Change Behavior</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>Reasonable Commitment Duration</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Data Processing Matches Policies</td>
<td></td>
</tr>
</tbody>
</table>

- **Data Removal**
  - If the data subject receives or has access to a record of requested changes.
  - If the data subject removes all data relating to the commitment.

- **Record Change/Delete Data Upon Commitment End/Change.**
  - If the data subject makes any changes.
  - If the data subject removes all data relating to the commitment.

- **Commitment**
  - If the data subject removes all data relating to the commitment.

- **Commitment, changes pertaining to data processor & co-data controller.**
  - If the information sharing [by the data controller] with data processors or co-data controllers who aren't included in the terms of service.

- **Commitment, changes pertaining to data controller data use.**
  - If the observed data controller data use behavior mostly doesn't match the privacy policy in substantial ways.

- **Commitment, changes pertaining to data collection.**
  - If the observed data controller data processing behavior mostly doesn't match the privacy policy in substantial ways.

- **Commitment, changes pertaining to data collection & use for multiple options in the commitment.**
  - If the observed data controller data processing behavior mostly doesn't match the privacy policy in substantial ways.

### Table: Data Subjects' Commitments

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Score</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>10A</td>
<td>Commitment Termination &amp; Change Behavior</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>Reasonable Commitment Duration</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Data Processing Matches Policies</td>
<td></td>
</tr>
</tbody>
</table>

- **Data Removal**
  - If the data subject receives or has access to a record of requested changes.
  - If the data subject removes all data relating to the commitment.

- **Record Change/Delete Data Upon Commitment End/Change.**
  - If the data subject makes any changes.
  - If the data subject removes all data relating to the commitment.

- **Commitment**
  - If the data subject removes all data relating to the commitment.

- **Commitment, changes pertaining to data processor & co-data controller.**
  - If the information sharing [by the data controller] with data processors or co-data controllers who aren't included in the terms of service.

- **Commitment, changes pertaining to data controller data use.**
  - If the observed data controller data use behavior mostly doesn't match the privacy policy in substantial ways.

- **Commitment, changes pertaining to data collection.**
  - If the observed data controller data processing behavior mostly doesn't match the privacy policy in substantial ways.

- **Commitment, changes pertaining to data collection & use for multiple options in the commitment.**
  - If the observed data controller data processing behavior mostly doesn't match the privacy policy in substantial ways.
### 4 - LOCATION COMMITMENT REQUIREMENTS

<table>
<thead>
<tr>
<th>TEST #</th>
<th>Mo2B COMMITMENT</th>
<th>SAFE &amp; RESPECTFUL COMMITMENT ATTRIBUTE</th>
<th>WHAT'S BEING MEASURED</th>
<th>GDPR MAP</th>
<th>CCPA/CPRA MAP</th>
<th>DATA USED TO MEASURE</th>
<th>EXPERTISE NEEDED TO EVALUATE</th>
<th>BEST PRACTICE (SCORE = +1)</th>
<th>PASSING BEHAVIORS (SCORE = 0)</th>
<th>FAILING BEHAVIORS (SCORES -1 to -3)</th>
</tr>
</thead>
<tbody>
<tr>
<td>LC1</td>
<td>Location Commitment - Browser Level</td>
<td>All</td>
<td>If the website uses browser level location tracking &amp; consent.</td>
<td>↑</td>
<td>↑</td>
<td>(3.140 (w)): Precise geolocation is treated as &quot;sensitive PII&quot;. May be less right to limit use to what is necessary to perform the services or provide the goods reasonably expected by an average consumer.</td>
<td>UX Expert</td>
<td>No use of browser level location tracking &amp; consent.</td>
<td>Use of browser level location tracking &amp; consent.</td>
<td>Use of browser level tracking &amp; location consent. (-3)</td>
</tr>
<tr>
<td>LC2</td>
<td>Location Commitment - data controller Level</td>
<td>(5) Private by Default</td>
<td>If the site automatically determines location without data subject permission.</td>
<td>=</td>
<td>☒</td>
<td>Not a violation. Not a lawful processing of personal data.</td>
<td>UX Expert</td>
<td>Use of browser level location tracking &amp; consent.</td>
<td>Use of browser level location tracking &amp; consent.</td>
<td>Use of browser level tracking &amp; location consent. (-3)</td>
</tr>
</tbody>
</table>
### 5 - ACCOUNT CREATION COMMITMENT REQUIREMENTS

<table>
<thead>
<tr>
<th>TEST #</th>
<th>MEASUREMENT</th>
<th>WHAT'S BEING MEASURED</th>
<th>GDPR MAP</th>
<th>CCPA/CPRA MAP</th>
<th>DATA USED TO ASSESS</th>
<th>USER REQUIRED TO TEST</th>
<th>BEST PRACTICE (SCORE = +1)</th>
<th>FAILING BEHAVIORS (SCORES = -1 to -3)</th>
</tr>
</thead>
<tbody>
<tr>
<td>MM1</td>
<td>Account Creation Commitment</td>
<td>Plain text fields in password/pin creation</td>
<td>x</td>
<td>x</td>
<td>Not Included</td>
<td>Not Included</td>
<td>Not Included</td>
<td>Collected as plain text (-3)</td>
</tr>
<tr>
<td>MM2</td>
<td>Account Creation Commitment</td>
<td>Plain text fields in password security questions</td>
<td>x</td>
<td>x</td>
<td>Not Included</td>
<td>Not Included</td>
<td>Not Included</td>
<td>Collected as plain text (-3)</td>
</tr>
<tr>
<td>MM3</td>
<td>Account Creation Commitment</td>
<td>&quot;Remember Me&quot; option presented to data subject</td>
<td>x</td>
<td>x</td>
<td>Not Included</td>
<td>Not Included</td>
<td>Not Included</td>
<td>Collected as plain text (-3)</td>
</tr>
<tr>
<td>MM4</td>
<td>Account Creation Commitment</td>
<td>&quot;Remember Me&quot; enabling</td>
<td>x</td>
<td>x</td>
<td>Not Included</td>
<td>Not Included</td>
<td>Not Included</td>
<td>Defaults to enabled (-3)</td>
</tr>
<tr>
<td>MM5</td>
<td>Account Creation Commitment</td>
<td>&quot;Remember Me&quot; disabling</td>
<td>x</td>
<td>x</td>
<td>Not Included</td>
<td>Not Included</td>
<td>Not Included</td>
<td>Website displays extremely sensitive personal information on the device without being logged in (-3)</td>
</tr>
<tr>
<td>MM6</td>
<td>Account Creation Commitment</td>
<td>Validates that no personal information is displayed when not logged in and &quot;not remembered&quot;</td>
<td>x</td>
<td>x</td>
<td>Not Included</td>
<td>Not Included</td>
<td>Not Included</td>
<td>Website continues to remember, recognize and personally respond to data subject (-1)</td>
</tr>
<tr>
<td>MM7</td>
<td>Account Creation Commitment</td>
<td>If too sensitive information is displayed/exposed when &quot;remembered&quot;</td>
<td>x</td>
<td>x</td>
<td>Not Included</td>
<td>Not Included</td>
<td>Not Included</td>
<td>Website displays extremely sensitive personal information on the device without being logged in (-3)</td>
</tr>
</tbody>
</table>