INTERNET
SAFETY
LABS

# Principles of Safe Software

| | |
|---|---|
| Version: | 1.1 |
| Date: | 12/13/22 |
| Editor: | Lisa LeVasseur |
| Authors: | ISL Software Safety Standards Panel |

## Abstract

Software products create Me2B relationships between users of software (Me-s) and the software developer business entity (B-s). The ISL software safety standard identifies safety risks and harms delivered in the context of this Me2B relationship.

Me2B relationships are comprised of a series of transactions that either deepen or diminish the Me2B relationship called, “Me2B Commitments”. Examples are cookie commitments, newsletter sign-up commitments, and account creation commitments. These are called commitments and not transactions because they entail the product "remembering" personal information about the user for some period of time.

ISL has identified the safety principles for such a Me2B commitment to be safe for people. All of the safety principles must be upheld for each Me2B commitment for a software product to be considered reasonably safe.

## Document Status

This document is a Specification produced by the ISL Software Safety Standards Panel.

## Copyright Notice

## Revision History

| VERSION | DESCRIPTION OF CHANGES |
|---|---|
| 1.0 | First release |
| 1.1 | Recategorized document to a Specification; updated to ISL company name. Removed Rules of Engagement. |
| | |
| | |
| | |

## Principle 1. Clear Data Processing Notice

There **must** be a readable data processing notice present in the software before any data collection or processing is performed as a part of this Me2B Commitment. [i]

## Principle 2. Viable Permission

### A. Understandability

The Data Subject **must** be able to easily understand the Me2B Deal required (quid pro quo) for this Me2B Commitment.

This requirement is the "knowledge" condition from Kim's description of the construction of [legal] consent. It relates closely to Attribute #1, the Clear Data Processing Notice. [ii]

### B. Freely Given

The Data Subject **must** have the ability to provide permission before any transaction carried out as a part of the Me2B Deal for this Me2B Commitment. There should be no element of coercion when seeking consent.

This is the "volition/voluntariness" portion of the construction of legal consent.[iii]

### C. Intentional Action

The Data Subject **must** provide a definitive, recorded affirmation of permission for the Me2B Deal required for this Me2B Commitment.

This is the "intentional manifestation of consent" portion of the construction of legal consent.

An affirmation or clear signal should provide enough information to provide a receipt of that transaction.[iv]

### D. Permission Flow to Data Processors (Transitive Permissions)

Data Subject's permissions **must** be shared with and upheld by all Data Processors.

## Principle 3. Identification Minimization

Any kind of identification performed **must** be proportional to the particular Me2B Commitment. Thus, the software **must** collect only the minimum set of identity attributes necessary to uniquely identify an individual as needed for the particular Me2B Commitment.[v]

## Principle 4. Data Collection Minimization

### A. Volunteered Data

The amount of Volunteered Data collected as a part of the Me2B Commitment **must** be appropriate to the Commitment.

### B. Observed Data

The amount of Observed Data collected as a part of the Me2B Commitment **must** be appropriate to the Commitment.

### C. Derived Data

The amount of Derived Data collected as a part of the Me2B Commitment **must** be appropriate to the Commitment.

## Principle 5. Private by Default

For the particular Me2B Commitment, any information shared **must** be private between the Data Subject and the Data Controller and any necessary Data Processors by default, without requiring any action by the Data Subject.

## Principle 6. Reasonable Data Use & Sharing Behavior

The observed Data Processing (with a particular focus on outbound data flow) **must** be appropriate / proportional for this particular Me2B Commitment.[vi]

## Principle 7. Data Processing Complies with Data Subject's Privacy Preferences & Permissions

The observed data processing behavior **must** comport with the Data Subject's preferences related to this Me2B Commitment.

## Principle 8. Data Processing Complies with Policies

The observed processing behavior (inclusive of collection) **must** match what is described in the Data Controller’s privacy policy and terms of service.

## Principle 9. Reasonable Commitment Duration

This particular Me2B Commitment's duration **must** match the expected or promised duration.

## Principle 10. Commitment Termination or Change Behavior

### A. Easy to End or Change Commitment

The Data Subject **must** be able to easily change or terminate the commitment.

### B. Record

The termination or change of the commitment **must** be recorded and provided to the Data Subject.

### C. Data Subject's Data Forgotten by Service

The Data Subject's data **must** be forgotten/deleted by all Data Controllers and Data Processors upon the termination of the commitment.

### D. Permission Change Flow to Data Processors

Permission changes [by the Data Subject] **must** flow down to all Joint-Data Controller and Data Processors, who must all take appropriate action (i.e. remove data).

[i] GDPR, Article 4 (2): "'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction"

GDPR, Chapter 1, Article 4 - Definitions, https://gdpr-info.eu/art-4-gdpr/

[ii] "Consent has a variety of meanings in the law, but it is typically a conclusion based upon the presence or absence of three conditions: an intentional manifestation of consent, knowledge, and volition/voluntariness."

Kim, Nancy S. Consentability (p. 9). Cambridge University Press. Kindle Edition.

"Consentability: Consent and Its Limits", Nancy S. Kim, 2019, Cambridge University Press.

[iii] GDPR Recital 42 "Burden of Proof and Requirements for Consent" https://gdpr-info.eu/recitals/no-42/

GDPR Recital 43 "Freely Given Consent" https://gdpr-info.eu/recitals/no-43/

[iv] ISO/IEC TS 27560 "Consent record information structure" is under development.

HL7 FHIR includes a Consent Resource with data structures https://www.hl7.org/fhir/consent.html

Kantara Initiative Consent Receipt Specification https://kantarainitiative.org/download/7902/

[v] GDPR Article 5(1)(c) "Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimization')" <add link>

See section 4.1.4 "Data Minimization" of the Kantara Report "Privacy & Identity protection in mobile Driving License ecosystems" https://kantarainitiative.org/download/7902/

[vi] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/