# Data Protection/Privacy Mapping Project Mission

The Data Protection/Privacy Mapping Project (the “**Project**”) facilitates consistent global comprehension and implementation of data protection with an open source mapping between ISO/IEC 27701 and global data protection and/or privacy laws and regulations.

# Principles

* Neutral – The project is not for profit and carries no affiliation or company-driven focus.
* Open – The data, infrastructure, and processes are available to all
* Consensus – Mapping data can at times be subjective, but consensus can be achieved through engagements with stakeholders
* Transparent – The operations and decision-making process for this project is transparent

# Scope

The Project aims to make the link between ISO/IEC 27001 and data protection regulatory requirements comprehensible to privacy professionals. It seeks to continuously improve and expand the data map between ISO/IEC 27701 and data protection laws and regulations, especially that of regulatory requirements. Initial mapping data is based on existing mapping between ISO/IEC 27701 and GDPR, and additional mappings were prepared by outside counsel for Microsoft between ISO/IEC 27701 and regulations from Australia, California, Canada, Brazil, Hong Kong, Singapore, South Korea, and Turkey.

**What?**

Crowdsourcing the mapping between ISO/IEC 27701 controls and various data protection requirements.

**Why?**

Data Protection regulatory requirements vary from jurisdiction to jurisdiction. With today’s global economy and shifting technology landscape, it is becoming increasingly difficult for organizations to manage data protection accountability efficiently and effectively. This mapping project leverages the universal data protection controls outlined by ISO/IEC 27701 to help organizations reconcile various laws and regulations with the common controls. Certification bodies, internal auditors and other stakeholders can then review the implementation of these controls to confirm accountability for the mapped regulations. Establishing a common understanding of the relationship between the ISO/IEC 27701 and data protection laws and regulations enables consistent interpretations and shared accountability among organizations globally. This can help strengthen data protection, technological solutions, and commerce.

**Microsoft’s role**

Microsoft initiated the Project by donating the initial data visualization code and regulatory mappings with ISO/IEC 27701 except the mapping with GDPR. The intention of publishing the content to open source is to stimulate international cooperation within the global privacy community and to improve the reliability and consistency of privacy practice. Microsoft will initially act as one of the Data Curators and Code Committers while the Project takes shape. Microsoft plans to transition away from the initial role of Data Curator as the Project matures.

**How?**

The Project encourages mapping contributions from data protection experts. The Data Curators will assess whether to accept, reject, or amend those contributions. Contributions that are accepted (with or without amendments) are then posted publicly with attribution for the public to review and consume. Contributions that are rejected are published separately with explanation from data curators within the site for future reference.

**Future efforts could focus on further topics such as the following examples:**

* Mapping Quality: Improve comprehensiveness, integrity and accuracy of the mapping
* Mapping Scope: Add new mappings
* Multilingual Capability: Enable multi-language capability both for mapping and consumption of data
* Improve User Interface: Include attribution of mapping source and time stamp
* Additional Data Visualization and Analytics
* Simplify Data Export

The ordering and completion of this projected work and effort applied will depend entirely on the community and their interests.

# Governance

**Processes**

The project undertakes four main operations in support of the stated goals and scope. Those processes are listed here in rough execution order:

**Consume**

The general expectation is that most users for the Project will only consume the data without making contribution. Users may use and download all or part of the mapping data for their own analysis under MIT license. Please note that the mapping data does not expose the full content of ISO/IEC 27701, which is the heart of the Project. Proper consumption of the project content requires acquisition of the standard from ISO, IEC, national standard bodies, such as BSI, ANSI, JISC, or ABNT, or other authorized sellers.

**Value-added projects**

Users are encouraged to create derivative, value-added projects from the mapping data for commercial purposes under the licensing terms of the Project. Users shall cite and acknowledge the Project. As the mapping data will evolve over time, time stamp or continuous data synchronization may be necessary. Commercial use of the mapping content shall respect the copyrights of ISO/IEC.

**Curate**

The curation process is open and transparent. Data Curators work on data contributed by the data protection community to validate presented information. All deliberations, discoveries and discussions are recorded and made available for community inspection.

Initially this workflow will happen in one or more GitHub repositories using standard Pull Request workflows on human-readable and diff-able curation artifacts. The project should develop additional tools to supplement or supplant this flow to better support users who are not technically savvy but will always ensure full transparency.

At least initially, all curated data must be signed off by two or more Data Curators after a due consideration of data quality. This is in the interest of working through thought and mechanical processes and developing a common understanding of the data and determining what is admissible. Disagreement in what is admissible should be resolved through consensus among Data Curators. While the voting process can be used to resolve such dispute, it is intended to be a procedure of last resort.

**Contribute**

Contribution from the data protection community is the most important activity for this project. All contributions are welcomed. Contributions may include correction or improvement of existing mappings, new mappings, and code contribution. Due to the nature and spirit of open source projects, all contributors must be either individually identifiable or representing an organization.

# Roles

**Data Curator**

A Data Curator is akin to a project maintainer or committer in typical open source projects. Data Curators have “write” permissions to the curation repository and are ultimately responsible for admitting data to the data repository. A Data Curator is responsible for data quality control, integrity and accuracy. The role requires reasonable domain context to enable issue identification and resolution. The role also requires technical expertise in running the necessary tools used to manage the project. Each curator must be, and be seen to be, neutral and impartial.

New Data Curators are nominated and approved by existing curators based on their merits and prior contributions. The role relates to an individual expert, an organization or a position in an organization. Under no circumstances, shall a Data Curator be held responsible for any errors or other flaws in the data merged into the service.

The current Data Curators are: Lanx Goh, Eric Lachaud, and Alex Li on behalf of Microsoft

**Data Contributor**

A Data Contributor for the Project is like a contributor on any other open source project – they identify bugs or improvements, fork the repo and contribute a pull request with their changes. For data contributors, this could be a small change (e.g., spelling correction or URL link submission), a substantive change (e.g., mapping correction), or wholesale data mapping (e.g., providing data mapping for additional regulations). Contributors should, as with any other open source project, expect to substantiate the changes with background information and adequate explanation of correctness. Since most Contributors are unlikely to be knowledgeable users of GitHub, data contribution in the form of spreadsheet sent to the Data Curators will be accepted.

A serial contributor of quality data or code is a candidate to become a curator or code committer.

**Consumer**

A Data Consumer accesses the curated data. They understand that the data is provided “as-is” with no guarantees or warranties as to (a) the correctness of the data or (b) suitability for any particular purpose. All data is fully qualified as to its origin and any clarifications made and it is up to the consumer to decide whether to use the data at their own risk.

**Code Committer**

While the Project is focused on data, the project initially contains a modest amount of code to enable data import and data visualization. Upon the initial release of the project, code committership and data curatorship roles are integrated. But it is recognized that there is a distinct skill set that is required for a Code Committer and a Data Curator. Separation of roles may develop as the project evolve.

The current Code Committers are: Benjamin Wong, Jieying Chng, and Alex Li on behalf of Microsoft

**Removal from role**

In the unlikely event that a committer or curator becomes disruptive or falls inactive for an extended period of time, they may be removed from the role through an absolute majority vote of the remaining set of committers and curators. Committers and curators may resign at any time from the Project. Advance notice in case of resignation is encouraged to identify replacement.

# Voting

Most decisions within the project can be done through informal consensus and recorded in the appropriate public record. When a formal decision is required, for example, when electing committers/curators, a vote is held using the following process:

* A topic for voting is tabled by a Data Curator or Code Committer by notifying all other Curators and Committers.
* Once tabled, Data Curators may vote during an open voting period lasting no less than one working week. Voting will occur on an agreed to, mutually convenient, and open medium (e.g., email, GitHub issue, etc.)
* A minimum of two positive (+1) votes and no negative (-1) votes carries the topic. Note that negative votes must be substantiated.
* Abstention (0) votes do not affect the outcome.