# Data Protection Mapping Project How-To Guide

## Contacts:

Project Owner: Alex Li [alli@microsoft.com](mailto:alli@microsoft.com),

## Location:

GitHub Repo location: <https://github.com/microsoft/data-protection-mapping-project>

Public URL: <https://dataprotectionmapping.z21.web.core.windows.net>

## General overview:

The purpose of this project is outlined in the GitHub Readme file: <https://github.com/microsoft/data-protection-mapping-project/blob/master/README.md>. The Readme file outlines the rationale behind the project and how it intends to operate. This document explains how to navigate the user interface of the tool, describe the data structure for those who want to view and edit the mapping dataset, and explain how to run and host the app at your local machine.

## The User Interface

The user interface consists of two areas—one for adding and filtering relevant regulations and standards on the left (see figure 1); another to display the mapping on the right (see figure 2).

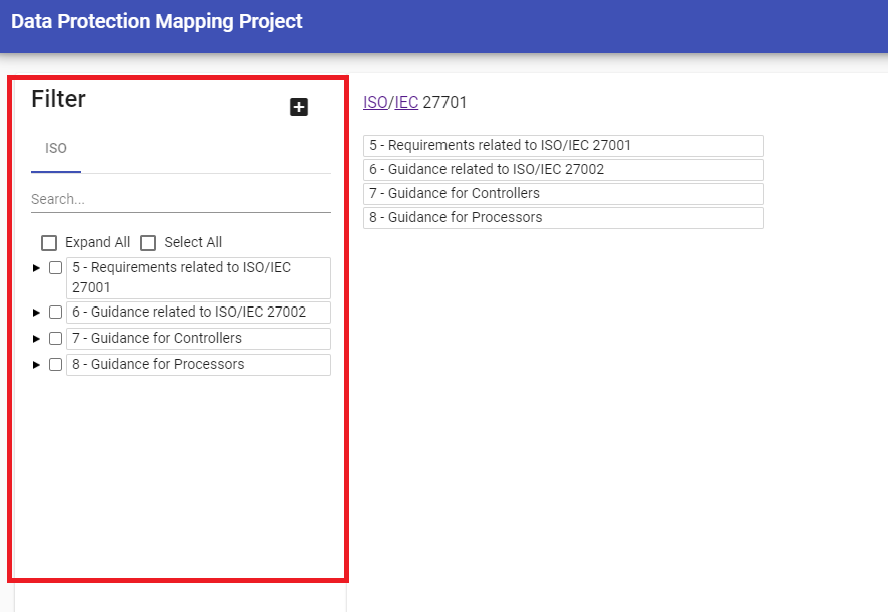


Figure : Filter Pane

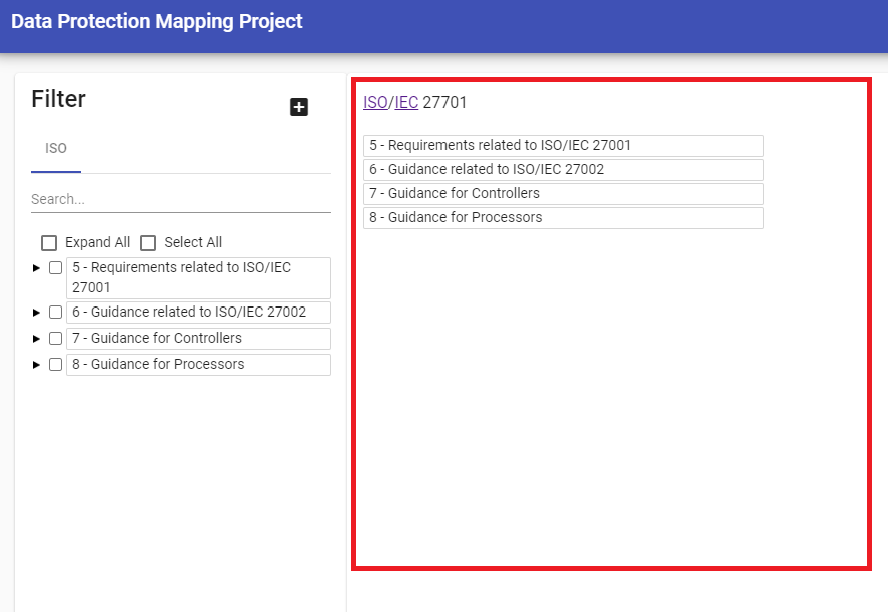


Figure Mapping Display

### Adding regulations for mapping display

The tool displays ISO/IEC 27701 on view permanently since all mappings orient around the standard. To see how regulations and requirements map to ISO/IEC 27701, click on the “+” icon on the top. A list of mapped regulations will be shown (see figure 3).

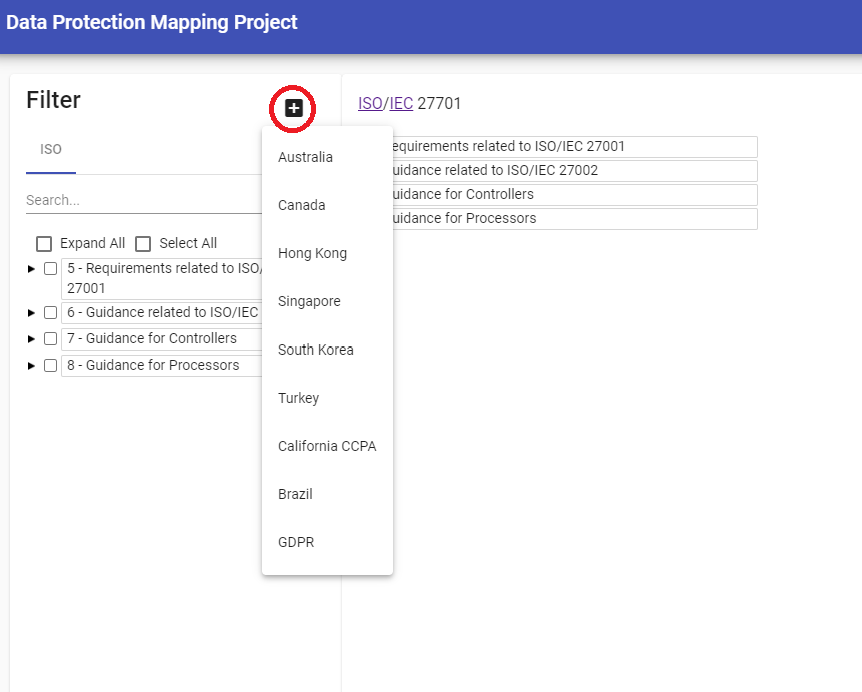


Figure Available regulations listed from filter pane

User may add up to two regulations to be added. For example, GDPR and California CCPA are added in the following screen shot (see figure 4). To dismiss any of the regulation from the mapping display, user can click on the “X” icon to the right of the regulation.

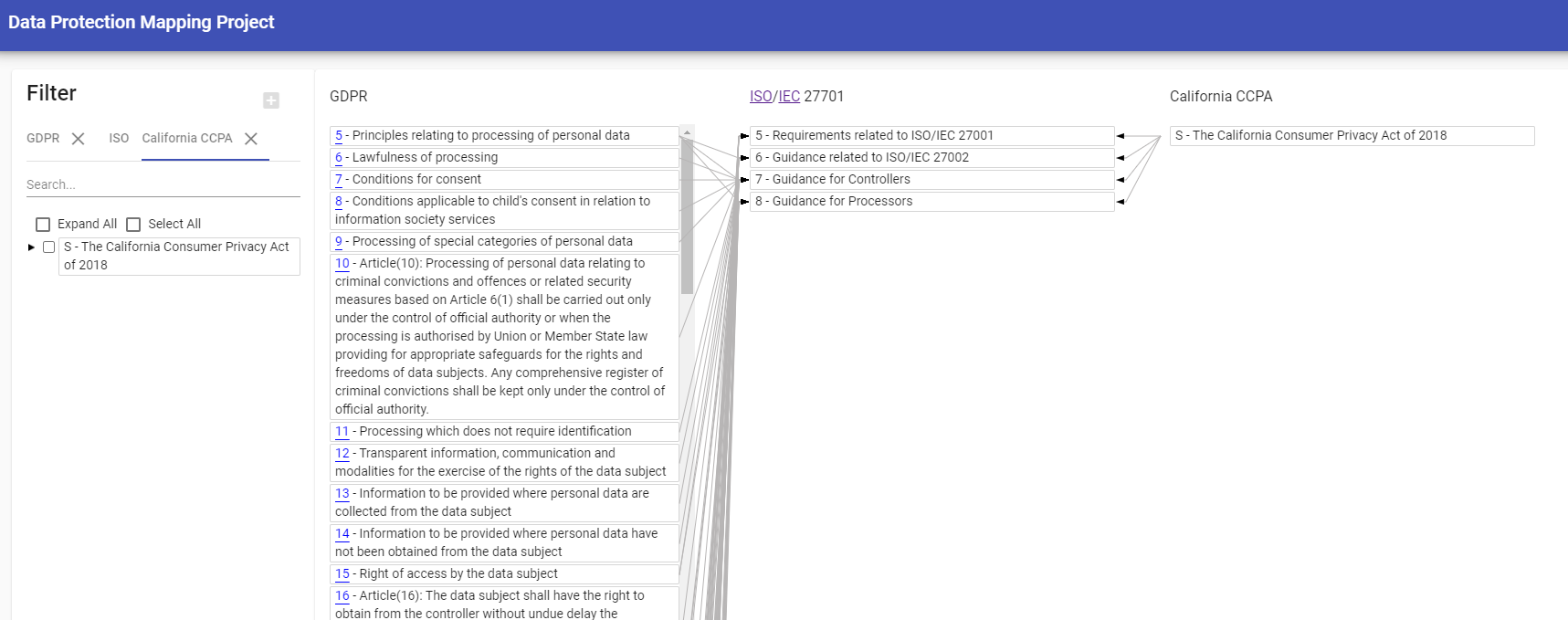


Figure Unfiltered view of GDPR and CCPA mappings

### Select the regulations or standard to filter

Since most regulations are rather lengthy and the corresponding mapping very extensive, filtering is necessary to make sense out of the mapping. To apply filtering, users need to select which regulation or ISO/IEC 27701 to use for filtering. The blue bar underneath the top left of the filtering pane indicates which regulation or standard to use for filtering. Click on any of the regulations or standard to select. Only one can be selected for filtering at a time. For example, we will start with filtering by GDPR (see figure 5).

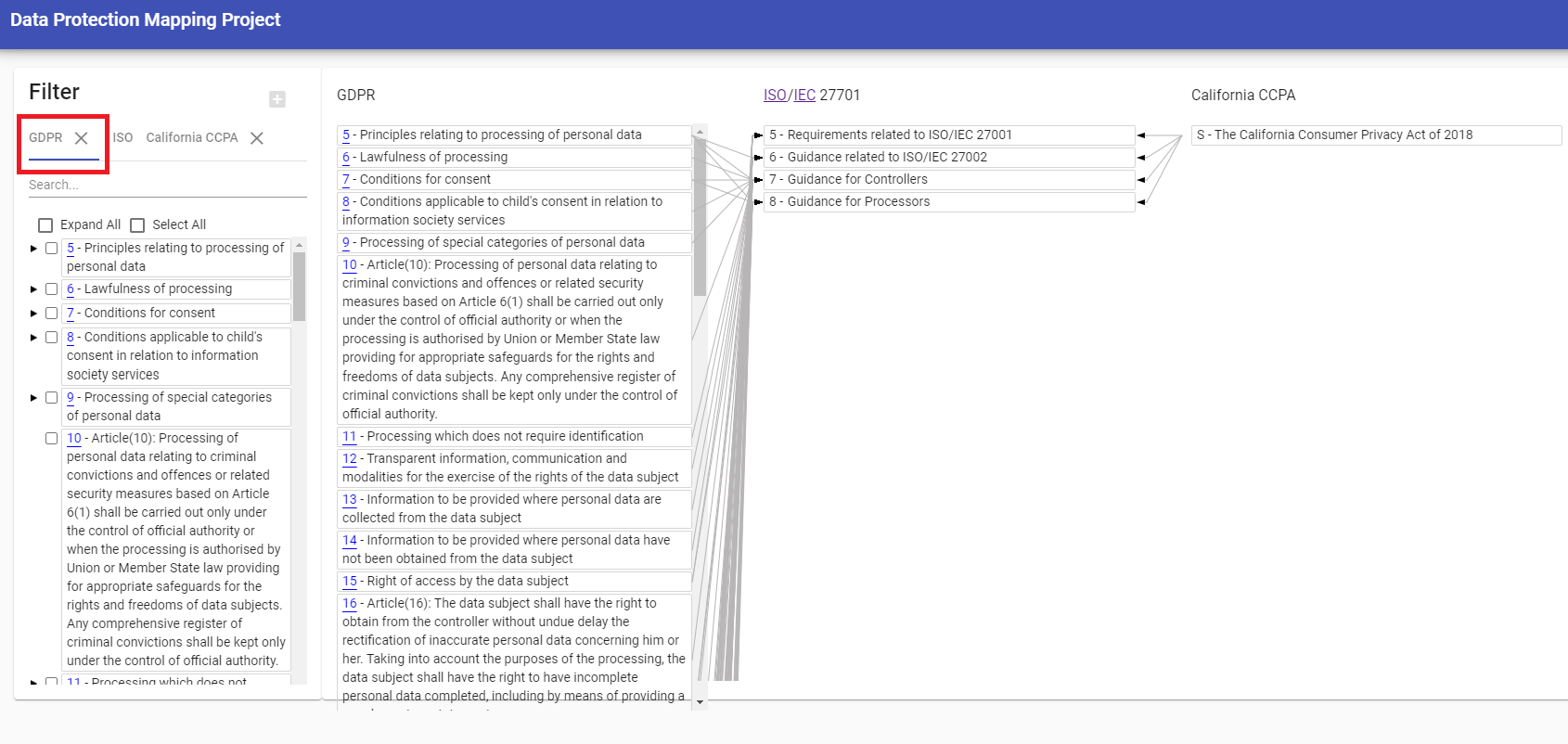


Figure GDPR selected for filtering

### Navigating the Hierarchy

User may select any part(s) of the regulations or standard to filter. Some regulations and standard contain nesting hierarchical structures. An arrow pointing to the right indicates that the corresponding part can be expanded to reveal sub-component. When there is no arrow, it indicates that component contains no sub-component with further detail. An arrow point down indicates that the component has been expanded. User can click on the arrows to expand or contract the hierarchy. For example, the following screen shot (figure 6) shows that Article 6 of GDPR expanded and that Article 6.1 of GDPR can further expand into more detailed components, while Article 6.2 is already at the most detailed level.

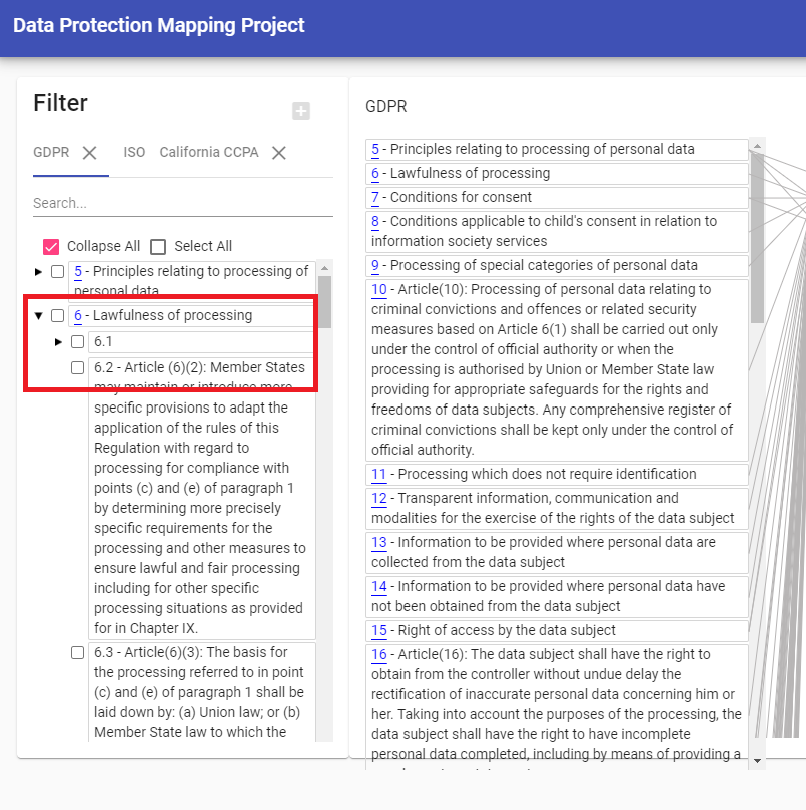


Figure Hierarchy of GDPR Article 6 and 6.1 shown

### Filtering

A checkbox toggles the filtering. User may filter by one or more components. Once the checkbox is checked, the mapping display on the right changes to reflect the new filtered view. In our example, we checked GDPR Article 6.2 (see figure 7). The yellow box reminds the user which regulation or standard is used for filtering.

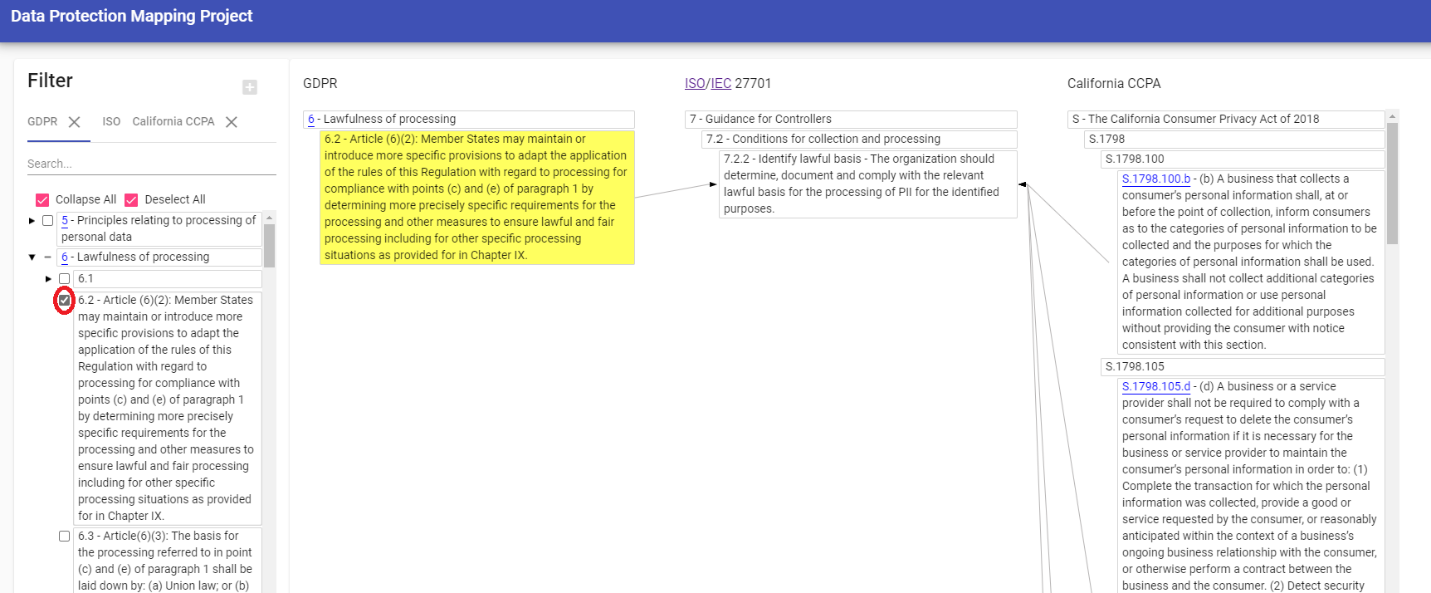


Figure GDPR Article 6.2 selected for filtering

### Highlighting

In case of complex mapping, user can select components on the mapping display to better view the mapping relationship. Selected component is shown in light blue. Mapping links are bolded to enable easy viewing. In the following example, we filtered by GDPR Article 15 which is mapped to many components of ISO/IEC 27701 and CCPA. Then we click on ISO/IEC 27701 clause 7.5.1 to see that it is mapped to GDPR Article 15.2 and CCPA 1798.110 b & c (see figure 8).

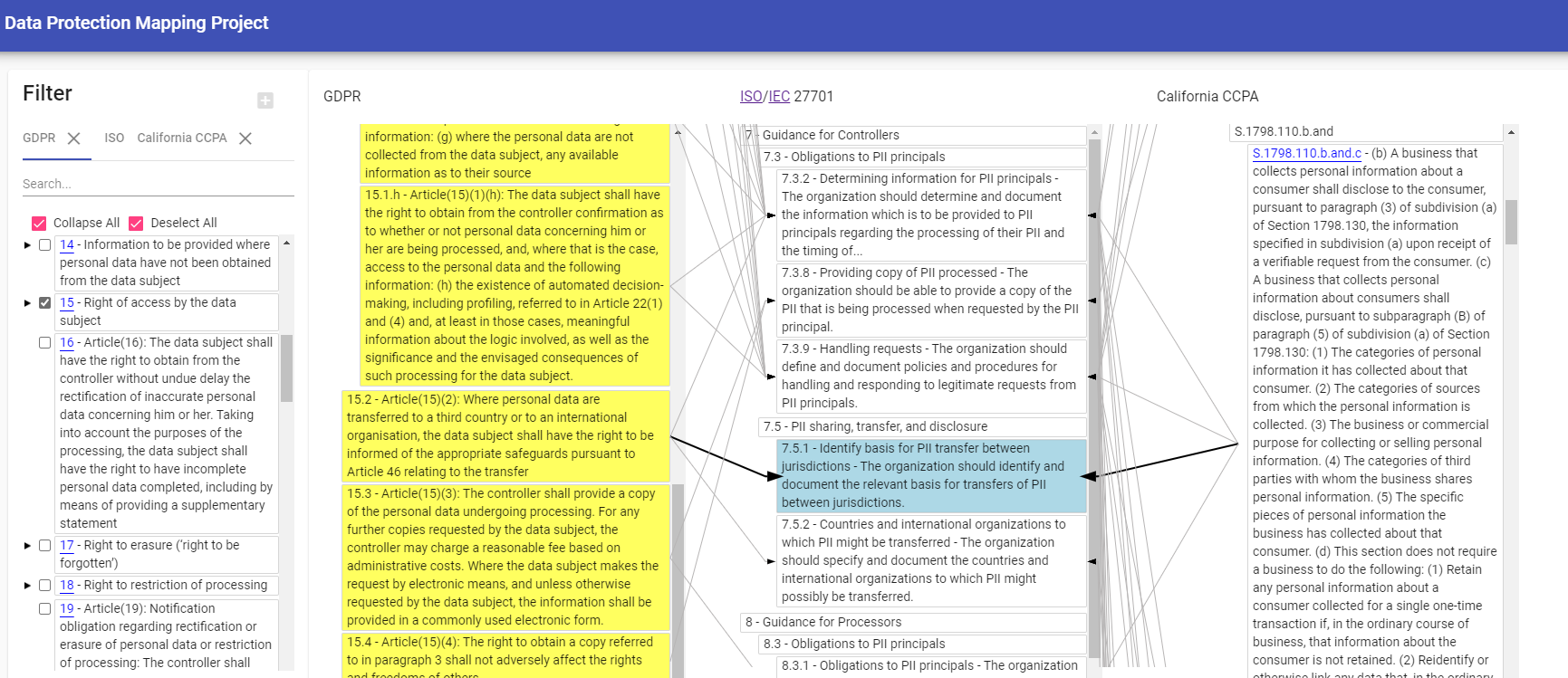


Figure ISO/IEC 27701 7.5.1 selected on the mapping display

### Search function

The filtering pane contains a text search function to help users find the appropriate filter. User starts with selecting the regulation or standard to be search and type in the text string for filtering. For example, typing in “child” under GDPR identifies Article 8. The text string is highlighted in yellow in the filter pane to aid the user (see figure 9). User still needs to toggle the checkbox to apply the filter. Clicking on the “x” on the right of the text search removes the text search.

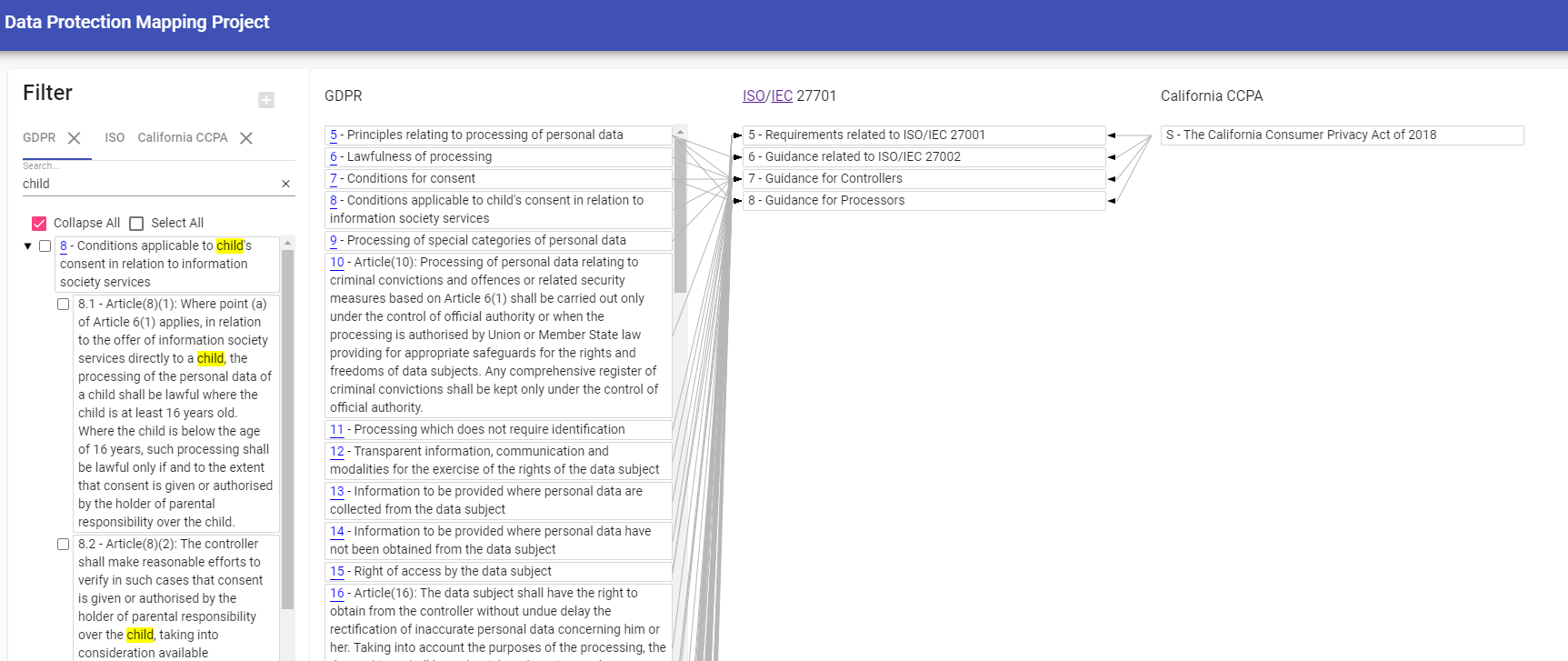


Figure search for the term "child" under GDPR

### In cases where is no matching component in ISO/IEC 27701

Some relevant regulatory components may not have a corresponding ISO/IEC 27701. This will make cross comparison inoperable. These components are highlighted in red. Components at a higher level of the hierarchy are highlighted in pink. The following example shows Australia Privacy Principle 9 with no corresponding match in the mapping (see figure 10).

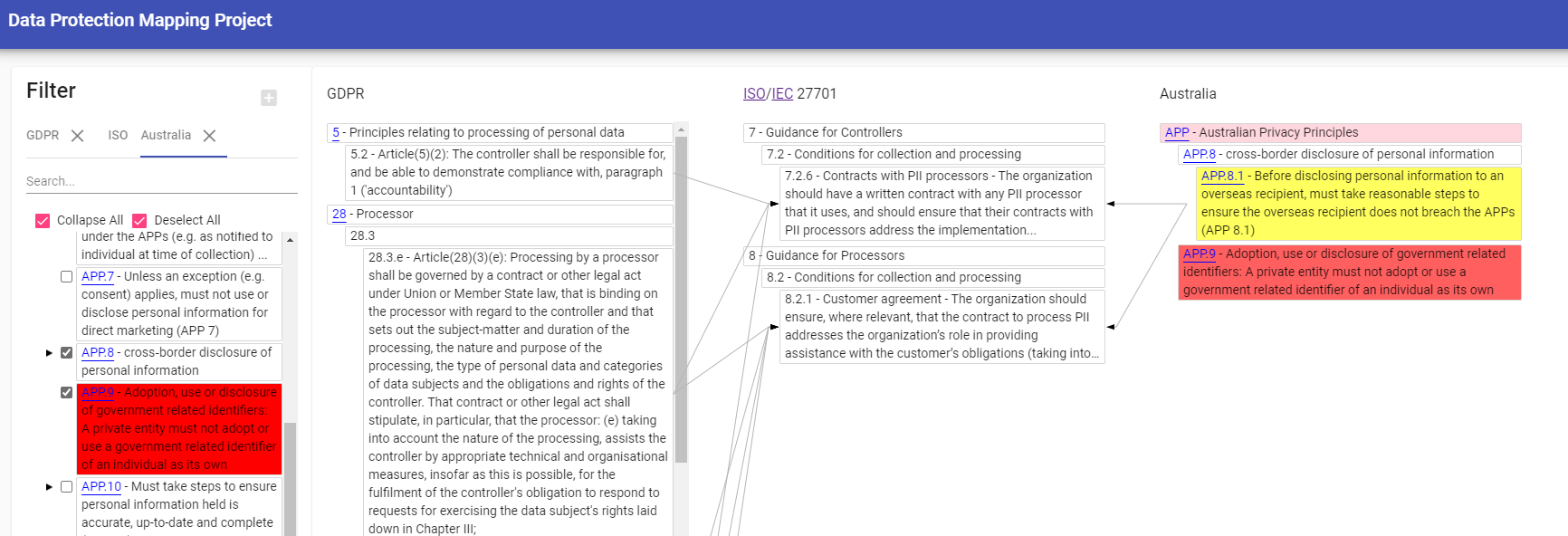


Figure Australian Privacy Principle 9 highlighted in red and Australian Privacy Principle highlighted in pink

Where possible, a URL link is provided at all levels to point users to the original regulatory text. All links are shown as blue underlined text in both the filter pane and the mapping display.

### Tree Node Colors:

* Red: Indicates the regulation node is unmapped. Unmapped nodes will always show because there is a potential that they should be mapped to the current filtered comparison.
* Pink: Indicates a descendent node is unmapped
* Yellow: Indicates the node is currently selected in a filter.
* Light Blue: Highlighted. Highlight nodes to see their connected links.

### Data Structure (for data contribution):

If you wish to contribute to the mapping database either by improving existing mapping or adding new regulations, the easiest way to do so is to send an updated spreadsheet to the project lead or directly from GitHub if you are technically proficient. The [Database.xlsx](https://github.com/microsoft/data-protection-mapping-project/blob/master/src/assets/database.xlsx) document has the following structure:

* Sheets – Each regulation is stored in its own sheet. The name of the sheet is what will show on the tab in the app.

It is expected that the change list will be the first sheet, and ISO 25572 regulation will be the second sheet.

* Columns:
  + id: A unique id for the article. These will be normalized into “dot” (.) delimited. Ex: A.1.b
  + section: The title of the article. This often includes the id and a short description.
  + body: The long description of the article, including implementation guidance.
  + hyperlink: A URL starting with “http” that points to the text in the regulation.
  + isolinks: Semicolon delimited list of ISO section ids.
* Id column structure:
  1. When imported, ids will be normalized to be dot delimited. Ex: A.1.b. They will be aggregated into a tree structure based on such that “1” would be a child of “A”, and “b” would be a child of “1”.

Example snippet from the Australia regulation sheet in Database.xlsx:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **id** | **section** | **body** | **hyperlink** | **isolinks** |
| APP | APP |  |  |  |
| APP.1 | APP.1 |  |  |  |
| APP.1.2 | APP.1.2 | Must take reasonable steps to implement practices, procedures and systems to ensure compliance with the APPs (APP 1.2) | https://www.legislation.gov.au/Details/C2018C00034/Html/Text#\_Toc506801611 | 5.2.3.a;5.2.4;5.4.1.3;6.2;6.4;6.5.2.1;6.11.2.5;6.13.1.1;6.15.1.3;6.15.2.1;6.15.2.3;7.2.5;7.3.1 |
| APP.1.4 | APP.1.4 | A privacy policy must contain the kinds of personal information collected and held, how and for what purposes it is collected, held, used and disclosed... | https://www.legislation.gov.au/Details/C2018C00034/Html/Text#\_Toc506801611 | 6.3 |
| APP.1.4.c | APP.1.4.c | Privacy policy must include purposes for which the entity collects, holds and uses personal information (APP 1.4(c)) | https://www.legislation.gov.au/Details/C2018C00034/Html/Text#\_Toc506801611 | 7.2.1 |

## Datasets:

There is no live database hosted. The app works of a static dataset and server. There are datasets.

* Private master dataset: A Database.xlsx file with all data including all mapping data.
* Cached public data: The app itself runs of a cached subset of public data, stored in the build and repository as a .json file which is easily read by the web app. This dataset is built from the private dataset using the import script.

### Updating the data in the system (For Project Administrators only)

1. Check-out the data repository containing the Database.xlsx.
   1. *git clone* <https://github.com/microsoft/data-protection-mapping-project>
2. Modify the data in the master dataset spreadsheet .xlsx.
3. Publish the changed xlsx back to the repository.
   1. *git add .*
   2. *git commit -m “XLSX change notes here”*
   3. *git push*
4. The automated build pipeline will import the data from the xlsx for public hosting.
5. Optional: To preview your changes locally, run the import script to convert the master dataset into the public dataset.
   1. *npm run import*

### Building the app (CI/CD, Production Preview):

Building the app requires Node and all the dev dependencies to be installed through Npm.

1. Check-out the app repository.
   1. *git clone* <https://github.com/microsoft/data-protection-mapping-project>
2. Navigate to the clone.
   1. *cd data-protection-mapping-project*
3. Install dependencies.
   1. *npm ci*
4. Build the app.
   1. *npm run build*

### Self-hosting the app (Local Preview):

Self-hosting is useful when developing the app or when previewing changes to the data. To self-host:

1. Check-out the app repository.
   1. *git clone* <https://github.com/microsoft/data-protection-mapping-project>
2. Navigate to the clone.
   1. *cd data-protection-mapping-project*
3. Install dependencies.
   1. *npm install*
4. Start the self-host server.
   1. *ng serve*
5. Navigate a web browser to the following URL.
   1. *localhost:4200*