Annotation Guidelines

- **Data Practice Category**
  - First Party Collection Information
    - how and why a service provider collects user information; and impact on service functionality if users refuse to provide information.
      - Application Scenarios / Functions
        - The application entity collects information for specified purposes, such as user profiling and data analysis, or to facilitate the provision of specific services.
      - Data Source
        - User-provided
          - Data that needs to be provided by the user themselves.
        - Obtained from Third Parties
          - Data obtained from third parties.
        - Cookie
          - Data obtained from Cookie.
        - Others
          - Data obtained from other.
      - Information Type
        - Identity information (name, ID card, birthday, etc.), device information (IMEI, MEID, AndroidID), etc.
      - Necessity
        - Must Provide
          - It is clear that providing this data is necessary to access this functionality.
        - Optional to Provide
          - Clearly states that user data is required for this scenario, and failure to provide it will restrict some functionalities within this scenario.
      - Sensitivity
        - Whether it is Personal Sensitive Information.

- Permission Acquisition
  - how and why a service provider obtains application permissions; and impact on service functionality if users refuse to grant permissions.
    - Application Scenarios / Functions
      - Permissions obtained by the application entity for specific purposes or to provide particular services and functionalities.
    - Permission Type
      - Fingerprint, facial ID, phone number, camera, storage, microphone, contacts, location, step count, floating window, notification bar, etc.
- Third Party Sharing/ Disclosure
  - how to share or transfer user information with the third party, publicly disclose it, or collect it by the third party.
    - Information shared by a third party | Information entrusted to a third party for processing
      - Sharing method
        - Non-SDK subject
        - Third-party SDKs
      - Third party
        - Company or APP
      - Purpose of sharing
        - Share data in certain usage scenarios or for specific reasons
      - Shared content
        - What part of the user's data is shared
      - Safety protection
        - Is there any clear indication of de-identification, anonymization, etc.
    - Transfer
      - Company merger, division, acquisition, asset transfer, change of operating entity or business relocation, reorganization or bankruptcy liquidation, personal information will be part of the transaction
    - Disclosure
      - App Asks Consent to Public
        - Disclosure to third-party individuals, organizations, and enterprises;

- Application does not ask for consent (judicial need, etc.)
  - Disclosure to administrative and judicial agencies
- Personal initiative to disclose and share
  - Internet or entities, Weibo, circle of friends, personal profile, etc.
- Others not solicited for direct disclosure

- Usage
  - ow user data is used, including: building data analysis models, personalized content recommendations or service models, automated decision-making models, etc.
    - User portrait
      - Build a data analysis model
    - Personalized advertising
      - Used to push advertisements to users
    - Content recommendation
      - Improved search, recommended content
    - Automated decision making
      - Processed automatically by the application, no actual natural person present.
- Data Retention
  - how long and where user information is stored.
    - Retention method
    - Retention location
      - China
      - Overseas
    - Storage period|time
    - Storage medium
- Data Security
  - how user information is protected.
    - Whether there is encryption technology such as anonymization
    - Whether there is a secure transmission protocol (HTTPs, etc.)

- Principles of Righteousness and Least
- Necessity
- principle of legality
- principle of safety prudence
- Is the least sufficient authorization principle
  other concerns

- Edit/Control
  - edit and control options available to users(e.g., modify and delete user information, turn off personalized ads or content recommendations, deactivate accounts, etc.
    - Turn off personalized ads
    - Disable content recommendations
    - Modify information
      - Add, delete, modify, check.
    - Revoke permissions
    - Log out of the account
    - Opt-out of subscriptions
    - Data migration
    - Create a backup copy
    - Disallow cookies
    - Publicize and share
      - The disclosure here focuses on curated published data, such as deleting published short articles, comments, etc.
    - Modification by administrators and other personnel
      - For some applications, the data management right belongs to the enterprise administrator

- Specific Audiences
  - practices that pertain only to a specific group of users (e.g., children, Europeans, or California residents)
    - specific area
      - Exclusive clauses in the privacy policy for people in specific regions, such as China, Zhejiang, Hong Kong, Europe, etc.

- special population
  - Minor
    - Whether to provide "Children's Privacy Protection Statement" and how to protect it, etc.
  - Deceased
    - Who Can Dispose and How
  - Laborer
- Contact Information
  - how contact service provider.
    - Contact customer service to modify data, consult questions, make complaints and other related content, and contact information of the enterprise, such as: email, telephone, etc.
- Policy Change
  - if and how users will be informed about changes to the privacy policy, and inform them what changes have been made.
    - Authorized
      - Data or software behavior after agreeing to the privacy policy. For example, it can be used without consent or cannot be used without consent.
    - Changes and Amendments
      - Change date
      - Whether the user will be explicitly notified and asked to authorize again
      - Change storage subject
      - Contents of change handling information
- Cease Operation
  - how user data will be handled when operation ceased.
    - Data processing guidelines after cessation of operations. Article 47 of the "Personal Information Protection Law" stipulates that when personal information processors stop providing products or services, they should delete personal information on their own initiative or at the request of individuals. The "Information Security Technology Personal Information Security Specification" requires that when personal information controllers stop their products or services, they should delete or anonymize the personal information they hold.

- **Special Marking**
  - Importantce
    - Importantce designed to identify content within Special Markings that contains explicit topic information, potential Risk, and Sensitive personal data.
      - All content deemed to require an abstract can be marked with this tag, even if it does not belong to the above categories. Example: If a sentence requires an abstract but does not belong to the above tags, only mark <important>. If a certain sentence belongs to the above tags, there are sentences that need to be summarized with category tags and <important> tags at the same time.
  - Risk
    - Risk is carefully designed to identify content that may pose potential threats to user information security, including situations that are inconsistent with legal regulations and are ambiguous or semantically unclear.
  - Sensitivity
    - Sensitivity refers to content that involves personal sensitive data, which, if disclosed or misused unlawfully, can easily lead to violations of an individual's dignity or pose risks to their personal and property safety. Sensitive personal information encompasses biometric data, religious beliefs, specific identities, health information, financial accounts, location tracking, and the personal details of minors under the age of fourteen.
- **Rewritten Sentences**
  - Rewrite the privacy policy sentences into short and easy-to-read declarative sentences, expressing the true intent of the privacy policy clauses in language that ordinary people can understand (using non-specialized vocabulary)

- **Note: (1) The subdivision attributes of all categories are only used for prompts. In other words, as long as the sentence or paragraph belongs to the important description of the corresponding class, no matter whether the sentence or paragraph belongs to the subdivision attribute displayed in the class, it can be marked as This category; (2) A text can correspond to multiple categories of labels; (3) The <important> label is independent of other labels and is used to identify whether a sentence belongs to a sentence that requires a summary. (4) Sentences that do not belong to the label category and do not require a summary do not need to be labeled. (5) Non-"important" and "risk" clauses do not need to be "rewritten".**