EpMap Annotation Manual for CBCMS+

Project Team: zhuangzhixian22s@ict.ac.cn

2025.3.15

Contents

1 Introduction

This annotation manual serves as a comprehensive guide for annotators tasked with annotating data for the Enhanced PDL Mapping Pipeline (EpMap). EpMap is a core component of CBCMS+, designed to map unstructured natural language legal texts into structured Policy Definition Language (PDL) formats. By converting complex legal clauses into machine-processable representations, EpMap enables the unified management of compliance policies across diverse legal frameworks and jurisdictions.

The primary objective of this manual is to ensure that annotators consistently and accurately identify and annotate PDL paths within legal text data. Each PDL field is meticulously detailed, providing definitions, annotation rules, practical examples, and common pitfalls to avoid. This structured approach enables annotators to systematically extract key elements from legal texts, such as roles, security measures, data subject rights, and jurisdiction-specific requirements.

Through this process, EpMap bridges the semantic gap between human-readable legal texts and machine-processable formats. It lays the foundation for high-quality training data, enabling the pipeline to achieve superior flexibility, accuracy, and efficiency. This manual is essential for maintaining annotation consistency and ensuring that EpMap meets its goal of supporting multi-jurisdictional compliance in global software systems.

2 Annotation Guidelines

2.1 Condition -> Role -> Controller

- **Definition:** This field identifies the "Controller," an entity that determines the purposes and means of data processing.
- **Annotation Rules:**
  (a) Look for explicit mentions of "Controller" or synonymous terms (e.g., "data controller," "data owner").
  (b) Ensure the entity is responsible for deciding how the data is processed.
- **Example:**

  Original Text: "The data controller determines the purposes of data processing."
  Annotation: `Condition -> Role -> Controller`

- **Common Mistakes:**
  – Do not annotate entities acting on instructions as "Controller" (e.g., processors).

2.2 Condition -> Role -> Processor

- **Definition:** This field identifies the "Processor," an entity that processes data on behalf of the controller.
- **Annotation Rules:**
  (a) Look for mentions of "Processor" or similar terms (e.g., "data processor").
  (b) Ensure the entity processes data based on the controller's instructions.
- **Example:**

  Original Text: "The processor acts on behalf of the controller."
  Annotation: `Condition -> Role -> Processor`

- **Common Mistakes:**
  – Do not annotate independent decision-makers as "Processor."

2.3 Condition -> Role -> Joint Controller

- **Definition:** This field identifies the "Joint Controller," an entity that, jointly with others, determines the purposes and means of data processing.
- **Annotation Rules:**
  (a) Look for terms like "Joint Controller" or phrases indicating shared decision-making responsibilities.

(b) Ensure multiple entities are involved in deciding data processing purposes and means.

- **Example:**

  Original Text: "The two parties act as joint controllers in determining processing activities."
  Annotation: `Condition -> Role -> Joint Controller`

- **Common Mistakes:**

  – Do not annotate a single decision-maker as "Joint Controller."

2.4 Condition -> Role -> Third Party

- **Definition:** This field identifies a "Third Party," an external entity not acting as a controller or processor.

- **Annotation Rules:**

  (a) Look for explicit mentions of "Third Party" or similar terms (e.g., "external entity").

  (b) Ensure the entity is not classified as a controller or processor.

- **Example:**

  Original Text: "Data can only be shared with a third party under strict conditions."
  Annotation: `Condition -> Role -> Third Party`

- **Common Mistakes:**

  – Do not annotate controllers or processors as "Third Party."

2.5 Condition -> Jurisdiction -> —

- **Definition:** This field specifies the jurisdictional scope related to legal or regulatory applicability.

- **Annotation Rules:**

  (a) Identify mentions of regions, countries, or legal frameworks indicating jurisdiction.

  (b) If no specific jurisdiction is mentioned, leave it as —.

- **Example:**

  Original Text: "This regulation applies to all EU member states."
  Annotation: `Condition -> Jurisdiction -> ---`

- **Common Mistakes:**

  – Avoid annotating geographic locations unrelated to legal applicability.

2.6 Condition -> Data Category -> —

- **Definition:** This field captures mentions of the type or category of data being processed.
- **Annotation Rules:**
  (a) Look for mentions of data categories such as "personal data," "sensitive data," or "health data."
  (b) If no specific category is mentioned, leave it as —.
- **Example:**

  Original Text: "Sensitive personal data must be handled with care."
  Annotation: `Condition -> Data Category -> ---`
- **Common Mistakes:**
  – Do not annotate activities or entities instead of data categories.

2.7 Condition -> Processing Purpose -> Marketing

- **Definition:** This field identifies data processing purposes related to "Marketing."
- **Annotation Rules:**
  (a) Look for mentions of activities aimed at advertising, promotions, or customer targeting.
  (b) Ensure the purpose aligns with marketing-related activities.
- **Example:**

  Original Text: "Data will be used for targeted marketing campaigns."
  Annotation: `Condition -> Processing Purpose -> Marketing`
- **Common Mistakes:**
  – Do not annotate non-marketing activities like compliance or research.

2.8 Condition -> Processing Purpose -> Compliance

- **Definition:** This field identifies data processing purposes related to "Compliance."
- **Annotation Rules:**
  (a) Look for mentions of legal obligations or adherence to regulations.
  (b) Ensure the purpose explicitly relates to satisfying legal requirements.
- **Example:**

  Original Text: "Data is processed to comply with applicable regulations."
  Annotation: `Condition -> Processing Purpose -> Compliance`
- **Common Mistakes:**
  – Do not annotate operational or service-related activities.

2.9 Condition -> Processing Purpose -> Research

- **Definition:** This field identifies data processing purposes related to "Research."
- **Annotation Rules:**
  (a) Look for mentions of activities aimed at scientific, market, or technological research.
  (b) Ensure the purpose is explicitly tied to research objectives.
- **Example:**

  Original Text: "The data is collected for academic research purposes."
  Annotation: `Condition -> Processing Purpose -> Research`

- **Common Mistakes:**
  – Do not annotate activities unrelated to research.

2.10 Condition -> Processing Purpose -> Service

- **Definition:** This field identifies data processing purposes related to "Service."
- **Annotation Rules:**
  (a) Look for mentions of activities aimed at providing or optimizing services.
  (b) Ensure the purpose is explicitly related to service delivery or improvement.
- **Example:**

  Original Text: "The data will be used to enhance customer service experience."
  Annotation: `Condition -> Processing Purpose -> Service`

- **Common Mistakes:**
  – Do not annotate marketing or compliance activities as "Service."

2.11 Condition -> Legal Basis -> Consent

- **Definition:** This field identifies "Consent" as the legal basis for data processing.
- **Annotation Rules:**
  (a) Look for explicit mentions of "Consent" or related terms (e.g., "user consent," "explicit agreement").
  (b) Ensure the text indicates that the data subject has provided clear and informed consent.
- **Example:**

  Original Text: "Processing is based on the consent of the data subject."
  Annotation: `Condition -> Legal Basis -> Consent`

- **Common Mistakes:**
  - Do not annotate implied or assumed consent without explicit mention.

2.12 Condition -> Legal Basis -> Contract

- **Definition:** This field identifies "Contract" as the legal basis for data processing.
- **Annotation Rules:**
  (a) Look for mentions of contractual obligations requiring data processing.
  (b) Ensure the processing is necessary for fulfilling a contract with the data subject.
- **Example:**

  Original Text: "Data processing is required to fulfill the contractual agreement."
  Annotation: `Condition -> Legal Basis -> Contract`
- **Common Mistakes:**
  - Do not annotate non-contractual obligations as "Contract."

2.13 Condition -> Legal Basis -> Legal Obligation

- **Definition:** This field identifies "Legal Obligation" as the legal basis for data processing.
- **Annotation Rules:**
  (a) Look for mentions of compliance with laws or regulatory requirements.
  (b) Ensure the obligation explicitly arises from legal or regulatory mandates.
- **Example:**

  Original Text: "Processing is necessary to comply with a legal obligation."
  Annotation: `Condition -> Legal Basis -> Legal Obligation`
- **Common Mistakes:**
  - Do not annotate voluntary compliance measures as "Legal Obligation."

2.14 Condition -> Legal Basis -> Legitimate Interests

- **Definition:** This field identifies "Legitimate Interests" as the legal basis for data processing.
- **Annotation Rules:**
  (a) Look for mentions of balancing organizational interests with individual rights.
  (b) Ensure the text explicitly references "legitimate interests."

- **Example:**

  Original Text: “The processing is necessary to pursue legitimate interests of the organization.”
  Annotation: `Condition -> Legal Basis -> Legitimate Interests`

- **Common Mistakes:**
  - Do not annotate scenarios without reference to balancing interests.

2.15 Condition -> Data Transfer Scope -> —

- **Definition:** This field specifies the scope of data transfer.
- **Annotation Rules:**
  (a) Identify mentions of data transfer regions or jurisdictions.
  (b) If no specific scope is mentioned, annotate as “—”.
- **Example:**

  Original Text: “Data transfers will involve multiple jurisdictions.”
  Annotation: `Condition -> Data Transfer Scope -> ---`

- **Common Mistakes:**
  - Avoid annotating unrelated geographic mentions.

2.16 Action -> Security Measures -> Encryption

- **Definition:** This field identifies “Encryption” as a security measure.
- **Annotation Rules:**
  (a) Look for mentions of encrypting data to ensure confidentiality.
  (b) Ensure the text specifies encryption as a security mechanism.
- **Example:**

  Original Text: “All personal data will be encrypted during transmission.”
  Annotation: `Action -> Security Measures -> Encryption`

- **Common Mistakes:**
  - Do not annotate unrelated security mechanisms as ”Encryption.”

2.17 Action -> Security Measures -> Pseudonymization

- **Definition:** This field identifies "Pseudonymization" as a security measure.
- **Annotation Rules:**
  (a) Look for mentions of pseudonymizing data to protect privacy.
  (b) Ensure the text references pseudonymization explicitly.
- **Example:**

  Original Text: "Pseudonymization techniques will be applied to sensitive data."
  Annotation: `Action -> Security Measures -> Pseudonymization`
- **Common Mistakes:**
  – Do not annotate anonymization as "Pseudonymization."

2.18 Action -> Security Measures -> Access Control

- **Definition:** This field identifies "Access Control" as a security measure.
- **Annotation Rules:**
  (a) Look for mentions of restricting access to authorized personnel.
  (b) Ensure the text references access control explicitly.
- **Example:**

  Original Text: "Access control policies will restrict data access to authorized users only."
  Annotation: `Action -> Security Measures -> Access Control`
- **Common Mistakes:**
  – Do not annotate security mechanisms unrelated to access control.

2.19 Action -> Security Measures -> Audit Logs

- **Definition:** This field identifies "Audit Logs" as a security measure.
- **Annotation Rules:**
  (a) Look for mentions of recording system or user activities.
  (b) Ensure the text specifies audit logs explicitly.
- **Example:**

  Original Text: "Audit logs will be maintained to track system access and activities."
  Annotation: `Action -> Security Measures -> Audit Logs`
- **Common Mistakes:**
  – Do not annotate general monitoring as "Audit Logs."

2.20 Action -> Security Measures -> Data Masking

- **Definition:** This field identifies “Data Masking” as a security measure.
- **Annotation Rules:**
  (a) Look for mentions of masking data to prevent unauthorized access.
  (b) Ensure the text references data masking explicitly.
- **Example:**

  Original Text: “Data masking will be used to obfuscate sensitive information.”
  Annotation: `Action -> Security Measures -> Data Masking`
- **Common Mistakes:**
  – Do not annotate encryption or pseudonymization as ”Data Masking.”

2.21 Action -> Security Measures -> Testing

- **Definition:** This field identifies “Testing” as a security measure to ensure the system’s robustness.
- **Annotation Rules:**
  (a) Look for mentions of system testing or security testing processes.
  (b) Ensure the text references testing activities explicitly.
- **Example:**

  Original Text: “Regular security testing will be conducted to identify vulnerabilities.”
  Annotation: `Action -> Security Measures -> Testing`
- **Common Mistakes:**
  – Do not annotate general quality assurance or unrelated evaluations as “Testing.”

2.22 Action -> Security Measures -> Evaluation

- **Definition:** This field identifies “Evaluation” as a security measure to assess the effectiveness of implemented controls.
- **Annotation Rules:**
  (a) Look for mentions of security evaluations, audits, or assessments.
  (b) Ensure the text explicitly references evaluation activities.
- **Example:**

Original Text: “Annual evaluations of security controls will ensure compliance with standards.”
Annotation: `Action -> Security Measures -> Evaluation`

- **Common Mistakes:**
  - Do not annotate testing or implementation activities as “Evaluation.”

2.23 Action -> Data Subject Rights -> Access

- **Definition:** This field identifies the right of data subjects to access their personal data.
- **Annotation Rules:**
  (a) Look for mentions of granting data subjects access to their personal information.
  (b) Ensure the text explicitly references access rights.
- **Example:**

  Original Text: “Data subjects have the right to access their personal data upon request.”
  Annotation: `Action -> Data Subject Rights -> Access`

- **Common Mistakes:**
  - Do not annotate rights unrelated to accessing personal data.

2.24 Action -> Data Subject Rights -> Erasure

- **Definition:** This field identifies the right of data subjects to request erasure of their personal data.
- **Annotation Rules:**
  (a) Look for mentions of deleting or removing personal data upon a data subject’s request.
  (b) Ensure the text explicitly references the right to erasure.
- **Example:**

  Original Text: “The data subject can request the erasure of their personal data at any time.”
  Annotation: `Action -> Data Subject Rights -> Erasure`

- **Common Mistakes:**
  - Do not annotate temporary data suspension or access restrictions as “Erasure.”

2.25 Action -> Data Subject Rights -> Rectification

- **Definition:** This field identifies the right of data subjects to request corrections to their personal data.
- **Annotation Rules:**
  (a) Look for mentions of correcting or updating inaccurate personal data.
  (b) Ensure the text explicitly references the right to rectification.
- **Example:**

  Original Text: "Data subjects can request rectification of any inaccurate information."
  Annotation: `Action -> Data Subject Rights -> Rectification`

- **Common Mistakes:**
  – Do not annotate general data updates not requested by the data subject.

2.26 Action -> Data Subject Rights -> Restriction

- **Definition:** This field identifies the right of data subjects to restrict the processing of their personal data.
- **Annotation Rules:**
  (a) Look for mentions of limiting or suspending data processing upon the data subject's request.
  (b) Ensure the text explicitly references the right to restriction.
- **Example:**

  Original Text: "Data subjects may request restrictions on data processing during investigations."
  Annotation: `Action -> Data Subject Rights -> Restriction`

- **Common Mistakes:**
  – Do not annotate complete erasure requests as "Restriction."

2.27 Action -> Data Subject Rights -> Portability

- **Definition:** This field identifies the right of data subjects to request the transfer of their data to another entity.
- **Annotation Rules:**
  (a) Look for mentions of transferring personal data in a structured, commonly used format.
  (b) Ensure the text explicitly references data portability.
- **Example:**

Original Text: “Data subjects have the right to request portability of their personal data.”
Annotation: `Action -> Data Subject Rights -> Portability`

- **Common Mistakes:**
  - Do not annotate general access requests as “Portability.”

2.28 Action -> Data Subject Rights -> Object

- **Definition:** This field identifies the right of data subjects to object to the processing of their personal data.
- **Annotation Rules:**
  (a) Look for mentions of objections to data processing activities.
  (b) Ensure the text explicitly references the right to object.
- **Example:**

  Original Text: “The data subject may object to processing based on legitimate interests.”
  Annotation: `Action -> Data Subject Rights -> Object`

- **Common Mistakes:**
  - Do not annotate withdrawal of consent as “Object.”

2.29 Action -> Data Subject Rights -> Withdraw

- **Definition:** This field identifies the right of data subjects to withdraw their consent for data processing.
- **Annotation Rules:**
  (a) Look for mentions of withdrawing previously given consent.
  (b) Ensure the text explicitly references consent withdrawal.
- **Example:**

  Original Text: “The data subject can withdraw their consent at any time.”
  Annotation: `Action -> Data Subject Rights -> Withdraw`

- **Common Mistakes:**
  - Do not annotate general objections or restrictions as “Withdraw.”

2.30 Action -> Data Retention -> —

- **Definition:** This field captures mentions of data retention policies or timeframes.
- **Annotation Rules:**
  (a) Identify mentions of how long data is retained or stored.
  (b) If no specific retention period is mentioned, annotate as "—".
- **Example:**

  Original Text: "Data will be retained for as long as necessary to fulfill its purpose."
  Annotation: `Action -> Data Retention -> ---`

- **Common Mistakes:**
  – Do not annotate general data processing mentions unrelated to retention.

2.31 Action -> Compliance Requirements -> Minimization

- **Definition:** This field identifies "Minimization" as a compliance requirement to process only the necessary amount of data.
- **Annotation Rules:**
  (a) Look for mentions of limiting data collection or processing to what is strictly necessary.
  (b) Ensure the text explicitly refers to minimizing data use or collection.
- **Example:**

  Original Text: "Data minimization principles require collecting only the data necessary for processing."
  Annotation: `Action -> Compliance Requirements -> Minimization`

- **Common Mistakes:**
  – Do not annotate general efficiency requirements unrelated to data processing.

2.32 Action -> Compliance Requirements -> Purpose Limitation

- **Definition:** This field identifies "Purpose Limitation" as a compliance requirement to process data only for specified purposes.
- **Annotation Rules:**
  (a) Look for mentions of processing data strictly for predefined or agreed-upon purposes.
  (b) Ensure the text explicitly references purpose limitation.
- **Example:**

Original Text: “Data must be processed solely for the purposes it was originally collected for.”
Annotation: `Action -> Compliance Requirements -> Purpose Limitation`

- **Common Mistakes:**
  - Do not annotate general data restrictions unrelated to specific purposes.

2.33 Action -> Compliance Requirements -> Transparency

- **Definition:** This field identifies “Transparency” as a compliance requirement to ensure data processing practices are open and clear.
- **Annotation Rules:**
  (a) Look for mentions of providing clear information about data processing to individuals.
  (b) Ensure the text explicitly refers to transparency in data handling.
- **Example:**

  Original Text: “Transparency requires organizations to inform users about how their data is processed.”
  Annotation: `Action -> Compliance Requirements -> Transparency`

- **Common Mistakes:**
  - Do not annotate privacy notices that do not explicitly mention transparency.

2.34 Action -> Compliance Requirements -> Accuracy

- **Definition:** This field identifies “Accuracy” as a compliance requirement to maintain correct and up-to-date data.
- **Annotation Rules:**
  (a) Look for mentions of ensuring data accuracy and updates.
  (b) Ensure the text explicitly references accuracy in data handling.
- **Example:**

  Original Text: “Organizations must take measures to ensure data accuracy and correct errors promptly.”
  Annotation: `Action -> Compliance Requirements -> Accuracy`

- **Common Mistakes:**
  - Do not annotate requirements unrelated to maintaining data correctness.

2.35 Action -> Third Party Sharing -> —

- **Definition:** This field captures mentions of sharing data with third parties.
- **Annotation Rules:**
  (a) Identify references to data being shared with external entities.
  (b) If no specific details are mentioned, annotate as "—".
- **Example:**

  Original Text: "Data can only be shared with third parties under strict conditions."
  Annotation: `Action -> Third Party Sharing -> ---`

- **Common Mistakes:**
  – Do not annotate internal data transfers as "Third Party Sharing."

2.36 Action -> Breach Notifications -> Immediate

- **Definition:** This field identifies the requirement to notify affected parties immediately in case of a data breach.
- **Annotation Rules:**
  (a) Look for mentions of notifying stakeholders without delay after a breach is discovered.
- **Example:**

  Original Text: "Immediate notification is required in the event of a data breach."
  Annotation: `Action -> Breach Notifications -> Immediate`

- **Common Mistakes:**
  – Do not annotate delayed notifications as "Immediate."

2.37 Action -> Breach Notifications -> Within 72 hrs

- **Definition:** This field identifies the requirement to notify parties of a breach within 72 hours.
- **Annotation Rules:**
  (a) Look for specific references to the 72-hour timeframe for breach notification.
- **Example:**

  Original Text: "Organizations must notify regulators of data breaches within 72 hours."
  Annotation: `Action -> Breach Notifications -> Within 72 hrs`

- **Common Mistakes:**
  – Do not annotate other timeframes as "Within 72 hrs."

2.38 Action -> Breach Notifications -> Periodic Reporting

- **Definition:** This field identifies the requirement to periodically report breach incidents.
- **Annotation Rules:**
  (a) Look for mentions of regular or periodic reporting of breaches to regulators or stakeholders.
- **Example:**

  Original Text: "Periodic reporting of breach incidents is required for compliance."
  Annotation: `Action -> Breach Notifications -> Periodic Reporting`
- **Common Mistakes:**
  – Do not annotate one-time notifications as "Periodic Reporting."

2.39 Action -> Data Localization -> —

- **Definition:** This field identifies requirements for data to remain within a specified jurisdiction.
- **Annotation Rules:**
  (a) Look for mentions of data localization or restrictions on cross-border transfers.
  (b) If no specific details are mentioned, annotate as "—".
- **Example:**

  Original Text: "Data must be stored within the European Union to comply with regulations."
  Annotation: `Action -> Data Localization -> ---`
- **Common Mistakes:**
  – Do not annotate general storage policies unrelated to jurisdiction.

2.40 Liability -> Accountability -> Controller

- **Definition:** This field identifies the accountability of the controller in ensuring compliance.
- **Annotation Rules:**
  (a) Look for mentions of the controller's responsibilities in maintaining compliance.
  (b) Ensure the text explicitly attributes accountability to the controller.
- **Example:**

Original Text: "The data controller is accountable for ensuring data protection measures are implemented."
Annotation: `Liability -> Accountability -> Controller`

- **Common Mistakes:**
  - Do not annotate processors or third parties as "Controller."

2.41 Liability -> Accountability -> Processor

- **Definition:** This field identifies the accountability of the processor in ensuring compliance with regulatory or contractual obligations.
- **Annotation Rules:**
  (a) Look for mentions of the processor's specific responsibilities.
  (b) Ensure the text explicitly attributes accountability to the processor.
- **Example:**

  Original Text: "Processors must implement security measures to protect data as instructed by the controller."
  Annotation: `Liability -> Accountability -> Processor`

- **Common Mistakes:**
  - Do not annotate controllers or joint controllers as "Processor."

2.42 Liability -> Accountability -> Joint Controller

- **Definition:** This field identifies the accountability of joint controllers in shared decision-making and compliance.
- **Annotation Rules:**
  (a) Look for references to joint decision-making responsibilities between multiple entities.
  (b) Ensure accountability is shared among the controllers.
- **Example:**

  Original Text: "Both parties, as joint controllers, are accountable for data protection compliance."
  Annotation: `Liability -> Accountability -> Joint Controller`

- **Common Mistakes:**
  - Do not annotate a single controller or processor as "Joint Controller."

2.43 Liability -> Accountability -> Supervisory Authority

- **Definition:** This field identifies the supervisory authority responsible for overseeing compliance.
- **Annotation Rules:**
  (a) Look for mentions of a regulatory body or supervisory authority.
  (b) Ensure the text explicitly refers to oversight or enforcement responsibilities.
- **Example:**

  Original Text: "The supervisory authority is responsible for monitoring compliance with data protection laws."
  Annotation: `Liability -> Accountability -> Supervisory Authority`

- **Common Mistakes:**
  – Do not annotate general references to authorities without oversight responsibilities.

2.44 Liability -> Supervision Requirements -> Mandatory Reporting

- **Definition:** This field identifies mandatory reporting requirements for compliance monitoring.
- **Annotation Rules:**
  (a) Look for explicit mentions of mandatory reporting obligations.
  (b) Ensure the text specifies what needs to be reported and to whom.
- **Example:**

  Original Text: "Organizations are required to submit mandatory reports to the supervisory authority."
  Annotation: `Liability -> Supervision Requirements -> Mandatory Reporting`

- **Common Mistakes:**
  – Do not annotate voluntary reporting activities.

2.45 Liability -> Supervision Requirements -> Periodic Audits

- **Definition:** This field identifies the requirement for regular audits to ensure compliance.
- **Annotation Rules:**
  (a) Look for references to periodic or regular compliance audits.
  (b) Ensure the audits are tied to compliance or supervisory processes.

- **Example:**

  Original Text: “Periodic audits are required to ensure adherence to data protection regulations.”
  Annotation: `Liability -> Supervision Requirements -> Periodic Audits`

- **Common Mistakes:**
  - Do not annotate one-time inspections as ”Periodic Audits.”

2.46 Liability -> Supervision Requirements -> Incident Reporting

- **Definition:** This field identifies the requirement to report incidents to the relevant authorities.
- **Annotation Rules:**
  (a) Look for mentions of reporting data breaches or compliance incidents.
  (b) Ensure the text specifies the incident reporting process.
- **Example:**

  Original Text: “Incident reporting to the supervisory authority is mandatory within 72 hours.”
  Annotation: `Liability -> Supervision Requirements -> Incident Reporting`

- **Common Mistakes:**
  - Do not annotate routine reporting as ”Incident Reporting.”

2.47 Liability -> Data Protection Impact Assessment -> —

- **Definition:** This field identifies the requirement to assess the impact of data processing activities.
- **Annotation Rules:**
  (a) Look for references to data protection or impact assessments.
  (b) If no specific assessment details are mentioned, annotate as “—”.
- **Example:**

  Original Text: “A data protection impact assessment must be conducted for high-risk processing activities.”
  Annotation: `Liability -> Data Protection Impact Assessment -> ---`

- **Common Mistakes:**
  - Do not annotate general compliance measures unrelated to assessments.

2.48 Extension -> Custom Clauses -> Targeted Advertising Restrictions

- **Definition:** This field identifies restrictions on targeted advertising as a custom clause.
- **Annotation Rules:**
  (a) Look for mentions of limiting or prohibiting targeted advertising practices.
  (b) Ensure the text explicitly references targeted advertising restrictions.
- **Example:**

  Original Text: "The company must avoid targeted advertising using sensitive personal data."
  Annotation: `Extension -> Custom Clauses -> Targeted Advertising Restrictions`

- **Common Mistakes:**
  – Do not annotate general marketing practices as "Targeted Advertising Restrictions."

2.49 Extension -> Custom Clauses -> Financial Risk Assessment

- **Definition:** This field identifies the requirement for assessing financial risks as a custom clause.
- **Annotation Rules:**
  (a) Look for mentions of evaluating financial risks associated with data processing.
- **Example:**

  Original Text: "Financial risk assessments are required for high-value data transactions."
  Annotation: `Extension -> Custom Clauses -> Financial Risk Assessment`

- **Common Mistakes:**
  – Do not annotate general operational risks as "Financial Risk Assessment."

2.50 Extension -> Custom Clauses -> Data Protection Officer

- **Definition:** This field identifies the requirement to appoint a Data Protection Officer (DPO) as a custom clause.
- **Annotation Rules:**
  (a) Look for mentions of appointing or designating a Data Protection Officer.
  (b) Ensure the text explicitly references a DPO role and its responsibilities.

- **Example:**

  Original Text: "Organizations must designate a Data Protection Officer to oversee compliance with data protection laws."
  Annotation: `Extension -> Custom Clauses -> Data Protection Officer`

- **Common Mistakes:**
  - Do not annotate general mentions of compliance roles unrelated to DPOs.

2.51 Extension -> Custom Clauses -> Cookie Consent

- **Definition:** This field identifies requirements for obtaining consent for cookies and similar tracking technologies.
- **Annotation Rules:**
  (a) Look for mentions of user consent specifically related to cookies or tracking technologies.
  (b) Ensure the text refers to obtaining explicit or informed consent.
- **Example:**

  Original Text: "Websites must obtain explicit user consent before placing cookies on devices."
  Annotation: `Extension -> Custom Clauses -> Cookie Consent`

- **Common Mistakes:**
  - Do not annotate general references to user consent unrelated to cookies.

2.52 Extension -> Cross Border Compliance -> —

- **Definition:** This field identifies requirements related to cross-border compliance without specific details.
- **Annotation Rules:**
  (a) Look for mentions of compliance requirements for data transfers between jurisdictions.
  (b) If no specific details are provided, annotate as "—".
- **Example:**

  Original Text: "Organizations must ensure compliance with cross-border data transfer regulations."
  Annotation: `Extension -> Cross Border Compliance -> ---`

- **Common Mistakes:**
  - Do not annotate references to single-jurisdiction compliance.

2.53 Extension -> Sanctions -> Fines

- **Definition:** This field identifies monetary penalties imposed as sanctions for non-compliance.
- **Annotation Rules:**
  (a) Look for mentions of fines or monetary penalties for regulatory violations.
- **Example:**

  Original Text: "Non-compliance may result in fines of up to €20 million."
  Annotation: `Extension -> Sanctions -> Fines`

- **Common Mistakes:**
  – Do not annotate references to sanctions unrelated to monetary penalties.

2.54 Extension -> Sanctions -> Legal Proceedings

- **Definition:** This field identifies legal actions taken as sanctions for non-compliance.
- **Annotation Rules:**
  (a) Look for mentions of legal proceedings, lawsuits, or judicial actions against organizations.
- **Example:**

  Original Text: "Failure to comply may result in legal proceedings initiated by the supervisory authority."
  Annotation: `Extension -> Sanctions -> Legal Proceedings`

- **Common Mistakes:**
  – Do not annotate references to fines or non-legal disciplinary actions.

2.55 Extension -> Sanctions -> Operational Suspension

- **Definition:** This field identifies operational suspensions imposed as sanctions for non-compliance.
- **Annotation Rules:**
  (a) Look for mentions of suspending operations, services, or business activities as penalties.
- **Example:**

  Original Text: "Severe violations may lead to the suspension of business operations in the region."
  Annotation: `Extension -> Sanctions -> Operational Suspension`

- **Common Mistakes:**
  – Do not annotate temporary service interruptions unrelated to sanctions.

3 Acknowledgments

This manual has been designed to ensure consistent and high-quality annotations for EpMap. For questions or clarifications, contact the project team: zhuangzhixian22s@ict.ac.cn.