PROCESSING

PURPOSE The Processing stage involves data storage, access controls, and taxonomization to enable analysis and use.

Developing Storage Guidelines

1. Creating Backup Systems: Have you created backup and archival systems to guard against data inaccessibility and/or data loss?

- Key Stakeholders: Data Engineering

2. Removing or Deleting Data: Have you established data removal and/or deletion protocols?

- Key Stakeholders: Partner, Data Engineering

3. Managing and Retiring Devices: Have you established guidelines for retiring storage devices containing sensitive information?

- Key Stakeholders: Data Engineering

4. Periodically Reviewing Storage Measures: Have you instituted periodic reviews of data storage procedures and policies to ensure their continued validity and relevance?

- Key Stakeholders: Data Engineering, External Experts

Developing Storage Guidelines

5. Configuring IT Security: Have you deployed robust IT security measures to prevent unauthorized access, data breaches, data loss, and data misuse?

- Key Stakeholders: Data Engineering

6. Expert Consultation: Have you consulted internal and external data security experts?

- Key Stakeholders: Data Engineering, External Experts

7. Providing Security Training: Have you ensured that staff have been trained in the proper handling of likely data security situations?

- Key Stakeholders: Operations/HR

8. Developing a Crisis Communication Strategy: Have you developed a response plan in the event of a data breach or other critical data incident?

- Key Stakeholders: Partner, Marketing/Communications, Management

Establishing Internal Access & Security Protocols

9. Providing Tiered Access: Have you established tiered levels of data access for staff?

- Key Stakeholders: Data Engineering, Operations/HR

10. Establishing Password Protocols: Have you deployed password update and multi-factor authentication processes for individuals with data access?

- Key Stakeholders: Data Engineering

11. Sharing Security Best Practices: Are partner(s) adequately trained in security practices, e.g., creating strong passwords and securing server rooms?

- Key Stakeholders: Partner

12. Creating a Change History and Audit Trail: Have you deployed procedures for auditing and documenting who accesses data, when, and changes to data over time such as copies, transformations, and edits?

- Key Stakeholders: Partner, Data Engineering

13. Deploying Internal Processing Safeguards: Have you encrypted, anonymized, or pseudonymized potentially sensitive data, e.g., PII, to guard against reidentification during internal data processing?

- Key Stakeholders: Partner, Data Engineering

Categorizing, Classifying & Taxonomizing Data

14. Capturing Data Provenance: Have you taxonomized data and captured data provenance to enable comparison, categorization, and classification?

- Key Stakeholders: Data Engineering, Data Science/Analytics

15. Mapping and Aggregating Data: Have you, if necessary, mapped data from its originally collected format into the format necessary for analysis?

- Key Stakeholders: Data Engineering

16. Documenting Processing Assumptions: Have you documented the assumptions and choices that informed data cleaning and categorization processes?

- Key Stakeholders: Data Engineering

17. Preventing Incompatible Data Combination: Have you deployed mechanisms to mitigate the risks of aggregating or correlating incompatible datasets?

- Key Stakeholders: Data Engineering, Data Science/Analytics