



Illustrative Example of DPA Template (Abbreviated)

Below is an excerpt from one of many Gray Reed Advisory Services' DPA tools and templates that we use to customize our clients' privacy program support experience based on their industry sector, market footprint, and business operating model.

I. General Information:

- a) What is the purpose and scope of the data processing activity?
- b) Who is the data controller responsible for the processing activity?
- c) Are there any third-party data processors involved?

II. Data Collection and Processing:

- a) What types of personal data are collected and processed?
- b) How is the data collected (e.g., directly from individuals or third parties)?
- c) Where is the data collected (e.g., in-person, online Adobe form, third-party managed website)?
- d) Was consent received and by what means and where is the consent record stored?
- e) What is/are the bases for processing personal data (e.g., consent, public safety)?

III. Data Uses:

- a) How will the data be used (e.g., to determine eligibility for products or to sell services)?
- b) Will third parties have access and for what reason(s)?
- c) Will the data be sold or shared internally or externally by the organization?

IV. Data Minimization and Retention:

- a) Is personal data collection limited to what is necessary and relevant for the intended purpose?
- b) Have retention periods been established for different categories of personal data?
- c) Does a process exist to regularly review and securely delete personal data when it is no longer needed?

V. Individuals' Rights:

- d) How are individuals informed about their rights under the TDPSA?
- e) Is there a process in place to receive and fulfill individuals' requests to exercise their rights (e.g., access, rectification, erasure)?
- f) Are there procedures to verify the identity of individuals making such requests?

VI. Security Measures:

- a) What technical and organizational measures exist to ensure the security of personal data?
- b) Have data protection policies and procedures been established and communicated to employees?
- c) Are there regular Cyber or IT Security audits and vulnerability assessments?