TrustArc Privacy and Data Governance Controls Framework

TrustArc

BUILD

Design, establish, and manage a program to ensure effective governance, risk management, policies, processes, and accountability.

6 Standards / 24 Core Controls

FS1 **Integrated Governance**
Identify stakeholders. Establish program leadership and governance. Define program mission, vision, and goals.

- 1.1 Identify internal stakeholders. Establish program leadership and governance. Define program mission, vision, and goals.
- 1.2 Appoint a CPO, DPO, or other Privacy Leader.

FS2 **Risk Assessment**
Identify, assess, and classify data-related strategic, operational, legal, compliance, and financial risks.

- 1.3 Identify, assess, and classify data-related strategic, operational, legal, compliance, and financial risks.
  - 1.3.1 Define objective criteria for assessing risks to individuals, the data, and the organization.
  - 1.3.2 Complete a program-level risk assessment and develop privacy program priorities and an implementation plan aligned to the outcomes of that assessment.
  - 1.3.3 Ensure that Privacy by Design (PbD) is based on an inherent risk analysis and incorporates appropriate controls for mitigating such risks.
  - 1.3.4 Develop data security program priorities and an implementation plan aligned to the outcomes of the program-level risk assessment.
  - 1.3.5 Where planned data processing presents a high inherent risk of harm to individuals based on objective criteria for assessing risks to individuals, ensure that privacy impact assessments address existing and potential risks identified in the organization by evaluating the effectiveness of controls mitigating such risks.

FS3 **Resource Allocation**
Establish budgets. Define roles and responsibilities. Assign personnel.

- 1.4 Allocate appropriate resources to support the defined mission and vision, and to manage identified risks.
  - 1.4.1 Establish and maintain budgets for privacy program.
  - 1.4.2 Define privacy-related roles and responsibilities. Assign competent personnel and support their development.

FS4 **Policies and Standards**
Develop policies, procedures, and guidelines to define and deploy effective and sustainable governance and controls for managing data-related risks.

- 1.5 Develop policies, procedures, and guidelines to define and deploy effective and sustainable governance and controls for managing data-related risks.
  - 1.5.1 Ensure the scope of policies, procedures, and guidelines is clearly defined.
  - 1.5.2 Document and communicate updates to policies, procedures, and guidelines.
  - 1.5.3 Ensure that policies and standards are enforceable.

FS5 **Processes**
Establish, manage, measure, and continually improve processes for PIAs, vendor assessments, incident management and breach notification, complaint handling, and individual rights management.

- 1.6 Establish, manage, measure, and continually improve processes for evaluating third parties to ensure that they have appropriate privacy and data protection safeguards in place.
- 1.7 Establish, manage, measure, and continually improve processes for implementing and maintaining personal data processing inventory with data classification built in.
- 1.8 Establish, manage, measure, and continually improve processes for developing, implementing, and periodically testing the effectiveness of a personal data incident management and breach response plan.
- 1.9 Establish, manage, measure, and continually improve processes for assessing the inherent data processing risk for new, ongoing, and modified data processing based on objective criteria for assessing risks to individuals.
  - 1.9.1 Establish, manage, measure, and continually improve processes for completing privacy impact assessments (PIAs) to evaluate the effectiveness of controls mitigating such risks.
  - 1.9.2 Establish, manage, measure, and continually improve processes for implementing all necessary controls to mitigate risk to appropriate levels.
- 1.10 Establish, manage, measure, and continually improve processes for establishing, implementing, publicizing, and actively managing a privacy complaint-handling process, including alternative dispute resolution as needed.
- 1.11 Establish, manage, measure, and continually improve processes for establishing, implementing, and actively managing processes to honor individual rights such as access, correction, deletion, and data portability.

FS6 **Awareness and Training**
Communicate expectations. Provide general and contextual training.

- 1.12 Communicate about the value and risks associated with data as well as program and process expectations. Provide both general and contextual training, including professional certification training. Reinforce messages periodically.

IMPLEMENT

Define data needs, identify data processing risks, ensure the data processing is lawful, manage data flows and third parties, address individual rights, provide data security, data quality, and transparency.

8 Standards / 24 Core Controls

FS7 **Data Necessity**
Optimize data value by collecting and retaining only the data necessary for strategic goals. Leverage anonymization, deidentification, pseudonymization, and coding to mitigate data storage-related risks.

- 2.1 Optimize data value by collecting and retaining only the data necessary for strategic goals. Leverage anonymization, de-identification, pseudonymization, and coding to mitigate data storage-related risks.

FS8 **Use, Retention, and Disposal**
Ensure data is used only as legally permissible and solely for purposes that are relevant to and compatible with the purposes for which it was collected.

- 2.2 Ensure data is used solely for purposes that are relevant to and compatible with the purposes for which it was collected.
- 2.3 Keep data in identifiable form only as long as necessary for identified processing purposes of which individuals have been informed. If data are needed for a longer period of time for research- or optimization-related purposes, implement coding, pseudonymization, or similar mechanisms to limit the risk to individuals.
- 2.4 Ensure that all data processing is legally permissible, including any data disclosures to third parties.
- 2.5 Define and communicate retention periods for personal data used by the process or technology.

FS9 **Disclosure to Third Parties and Onward Transfer**
Preserve the framework standards and protections for data when it is transferred to third-party organizations and/or across country borders.

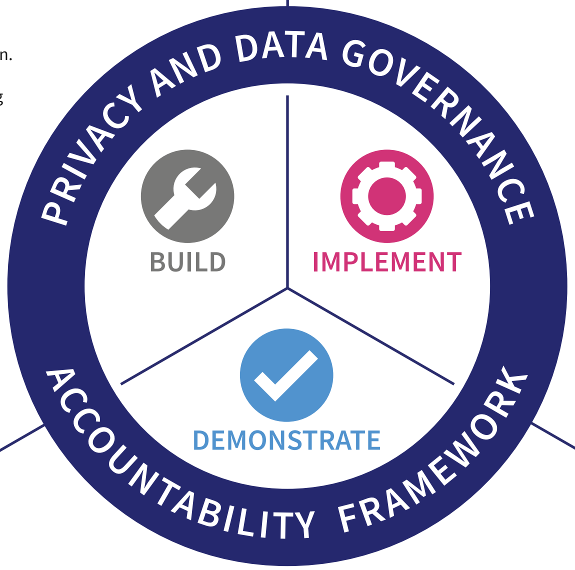
- 2.6 Assess vendors handling personal data for effective safeguards and controls.
- 2.7 Execute appropriate contracts with vendors supporting the process or technology or with any third parties.
- 2.8 Ensure personal data is adequately protected when transferred internationally, including transfers to third parties and vendors.

FS10 **Choice and Consent**
Enable individuals to choose whether personal data about them is processed. Obtain and document prior permission where necessary and appropriate, and enable individual to optout of ongoing processing.

- 2.9 Enable individuals to choose whether personal data about them is processed. Obtain and document prior permission (consent) where necessary and appropriate, and enable individual to opt-out of ongoing processing.
  - 2.9.1 Ensure consent is clear and conspicuous, freely given, and able to be withdrawn at any time.
  - 2.9.2 Ensure that evidence of consent can be produced at any time.
- 2.10 If the individual is a child (as defined by applicable law), obtain verifiable parental consent for the processing.
- 2.11 Provide mechanisms for individuals to easily opt-out of ongoing processing about them.

FS11 **Access and Individual Rights**
Enable individuals to access information about themselves, to amend, correct, and as appropriate, delete information that is inaccurate, incomplete, or outdated.

- 2.12 Enable individuals to access information about themselves, to amend, correct, and as appropriate, delete information that is inaccurate, incomplete, or outdated.
- 2.13 Enable individuals to rectify inaccurate personal data processed by the technology, process, or activity.
- 2.14 Where appropriate and in accordance with applicable law, enable individuals to delete personal data processed by the technology, process, or activity.
- 2.15 Enable individuals to request reasonable restrictions on uses or disclosures of personal data about them where such restrictions do not adversely affect the rights of others, do not require disproportionate efforts for the organization to implement, or where required by law.
- 2.16 Where reasonable and practicable, enable individuals to access information about themselves in a machine-readable or electronic format consistent with its intended use.



FS12 **Data Integrity and Quality**
Assure that data is kept sufficiently accurate, complete, relevant, and current consistent with its intended use.

- 2.17 Assure that data are kept sufficiently accurate, complete, relevant, and current consistent with its intended use.

FS13 **Security**
Protect data from loss, misuse, and unauthorized access, disclosure, alteration, or destruction.

- 2.18 Put in place administrative, physical, and technical safeguards to protect data from loss; misuse; and unauthorized access, disclosure, alteration, or destruction.
- 2.19 Conduct security risk assessments as required by the security program, and remediate areas of identified risk.

FS14 **Transparency**
Inform individuals about the ways in which data about them are processed and how to exercise their data-related rights.

- 2.20 Inform individuals about the ways in which data about them are processed and how to exercise their data-related rights, including those arising out of data-related incidents and breaches.
  - 2.20.1 Ensure information about data processing and individuals rights is clear and conspicuous.
  - 2.20.2 Ensure information about data processing and individuals' rights is provided before information is collected from individuals, at the time of collection, or as soon as practicable thereafter.

DEMONSTRATE

Monitor, evaluate, and report on compliance, control effectiveness, risk, and maturity.

2 Standards / 7 Core Controls

FS15 **Monitoring and Assurance**
Evaluate and audit effectiveness of controls and risk-mitigation initiatives.

- 3.1 Continually monitor and periodically evaluate program maturity, and periodically assess and audit the effectiveness of program controls and risk-mitigation initiatives.

FS16 **Reporting and Certification**
Demonstrate the effectiveness of your program and controls to management, the Board of Directors, employees, customers, regulators, and the public.

- 3.2 Select and implement mechanisms to demonstrate the effectiveness of your program and controls to management, the Board of Directors, employees, customers, regulators, and the public.
- 3.3 Establish a point of contact for direct cooperation with DPAs.
- 3.4 Consider demonstrating compliance by adhering to binding and enforceable codes of conduct.
- 3.5 Consider demonstrating compliance through certification, seals, and/or marks.
- 3.6 Consider demonstrating corporate data responsibility to customers and the public as part of the organization's corporate social responsibility and/or sustainability goals.
- 3.7 If your organization is a data-driven business, consider demonstrating data stewardship, ethics, and accountability as part of the value of the organizational brand value.