COSMOS
Navigate the Compliance Universe

Corporate Compliance Forms and Tools
Privacy Compliance Program Checklist

Below is a list of the key elements to use as part of a self-assessment of your organization's privacy program.

Compliance Program Element	Suggested Data Privacy Compliance Program Component	Complete
Standards and procedures	• Evidence that the organization's code of conduct reinforces a commitment to safeguarding privacy. • Evidence of the organization's data protection impact assessment program. • Evidence that privacy and related policies are examined periodically and take into consideration changes to the privacy risk—and related, broader IT/information security—landscape and wrongdoing perpetuated in the recent history pertaining to that policy. • Evidence of privacy breach response policies and protocols. • Evidence that departmental policies have been further contextualized to account for specific personal data flows. • Evidence that the company has a privacy communication plan that includes distribution of privacy policies.	☐ ☐ ☐ ☐ ☐ ☐
Governance, oversight, authority	• Evidence that privacy measures are incorporated into annual organizational goal setting and include appropriate follow-up. • Evidence that the annual report to senior leadership and the board on the data privacy compliance program includes the results of the organizational privacy risk assessment and consideration of related information security risks, results of internal audits, and incident trends. • Evidence of funding for the privacy program, including people, process, and technology.	☐ ☐ ☐
Due care in delegation of authority	• Evidence that privacy professionals demonstrate the right professional qualifications and expert knowledge of the data protection legal and regulatory environment. • Evidence of documented privacy roles and responsibilities, including, where applicable, adherence to regulatory requirements such as the General Data Protection Regulation (GDPR) and the role of the data protection officer.	☐ ☐

Communication and training	• Evidence of a privacy-specific learning and awareness plan, updated annually, reflecting the results of the organization's overall risk profile (e.g., GDPR, California Consumer Privacy Act, Health Insurance Portability and Accountability Act). • Evidence of the privacy-specific awareness program or process reflective of its unique organizational risk profile. • Evidence of privacy-specific awareness for middle/senior leadership as well as the board or similar senior leadership body.	☐ ☐ ☐
Auditing, monitoring, and reporting systems	• Evidence of the organization's data protection–specific third-party assessment program where the third-party relationship is assessed against the company's privacy and related information security policies, including, for example, data minimization, privacy by design, and a data protection impact assessment. • Evidence that data protection is a core component of the company's mergers and acquisitions assessment process.	☐ ☐
Incentives and discipline	• Evidence of the organization's data protection–specific disciplinary and incentive measures, including, for example, consequences for noncompliance with the company's acceptable use policy or privacy policy. Evidence that these measures apply across all ranks, including senior leadership.	☐
Response to wrongdoing and remediation	• Evidence that complaint, inquiry, and privacy breach response protocols are consistently followed through a privacy case management system or similar process. • Evidence that data privacy inquiries or complaints are addressed consistent with applicable privacy requirements, including timing as well as process (such as subject access rights requests). • Evidence that data incidents are addressed consistent with applicable law, such as the GDPR's 72-hour requirement, including root cause analysis and remedial measures such as control improvements, changes to systems, improvement of the existing data protection impact assessment process, and internal and/or external notifications consistent with applicable law.	☐ ☐ ☐
Risk assessment and continuous improvement	• Evidence that the company conducts a periodic (annual at minimum) data privacy risk assessment designed to identify changes to the organization's inherent privacy risks and responsive measures to prevent, detect, and respond to those risks. • Evidence that the company conducts an annual data protection compliance program assessment, which includes testing of program components and results of privacy audits, which inform recommended control enhancements. • Evidence that the organization's data protection impact assessment program includes periodic reassessment of systems and processes.	☐ ☐ ☐