Data Privacy Specialist/Privacy Officer

NICE Framework Reference	Oversee and Govern, OV-LGA-002, Privacy Officer/Privacy Compliance Manager
Functional Description	Develops, implements, advises on and administers organization privacy compliance program which supports requirements to safeguard personal private information (PPI).
Consequence of error or risk	Error, neglect, outdated information, lack of attention to detail or poor judgment could result in a compromise or breach of PPI, which, in addition to the potential individual consequences and liability, may result in significant fines levied for the breach, and loss of reputation and trust.
Development pathway	This role may be supported through technical or non-technical pathways that lead to an entry level role related to privacy/sensitive data management and progress to the policy advisor level. Individuals can further specialize in data security or policy analyst, or senior advisor.
Other titles	▪ Privacy officer ▪ Privacy compliance officer/manager
Related NOCs	2171 Information systems analysts and consultants 416X Policy and program researchers, consultants and officers (context dependent)
Tasks	▪ Interpret and apply laws, regulations, policies, standards, or procedures to specific privacy issues ▪ Conduct periodic impact assessments and ongoing compliance monitoring activities to identify compliance gaps and/or areas of risk to ensure privacy concerns, requirements and responsibilities are addressed ▪ Establish and maintain a mechanism to track access to information within the purview of the organization and as required by law to allow qualified personnel to review or receive such information ▪ Establish and implement an internal privacy audit program, and prepare audit reports that identify technical and procedural findings, and privacy violations, and recommend remedial solutions ▪ Provide advice and guidance on laws, regulations, policies, standards, or procedures to management, personnel, or key departments ▪ Ensure compliance with privacy and cybersecurity laws, regulations, and policies, and consistent application of sanctions for failure to comply with stated measures for all personnel in the organization ▪ Initiate, facilitate and promote activities to foster privacy awareness within the organization that include the collection, use and sharing of information ▪ Monitor advancements in privacy enhancing technology and ensure the use of technologies complies with privacy and cybersecurity requirements, including the collection, use and disclosure of information ▪ Review the organization's network security plans and projects to ensure that they are consistent with privacy and cybersecurity goals and policies ▪ Collaborate with legal counsel and management to ensure the organization has and maintains appropriate privacy and confidentiality consent, authorization forms, and relevant materials are compliant with legal practices and requirements

	▪ Develop, deliver, and oversee privacy training material and awareness activities	
Required qualifications	Education	Post-secondary education in an applicable field (e.g.; Business Administration, Law, Political Science, Social Sciences or equivalent)
	Training	Specialized training in data privacy and security, cybersecurity foundations, privacy impact analysis, privacy legislation and compliance
	Work experience	Previous training and experience (2-3 years) in policy analysis role related to security or privacy typically required for entry level role
Tools & Technology	▪ Privacy and information legislation and policies ▪ Compliance requirements ▪ Reporting mechanisms and templates ▪ Privacy impact assessments/statements of sensitivity ▪ Threat and risk assessments ▪ Data and information requirements ▪ Privacy assessment tools and methodologies	
Competencies	KSAs applied at the basic level: ☐ A working knowledge of cybersecurity principles and elements ☐ Technical knowledge to understand data security and integrity, security requirements, and the functional and technical design of networks and system, and cybersecurity solutions ☐ Data security conceptions and functions, analysis methodologies, testing, and protocols ☐ Cybersecurity program management, measures and monitoring KSAs applied at an advanced level: ☐ Threat and risk assessment (focused on privacy / data privacy security) ☐ Domestic and international laws, regulations, policies, and procedures; ☐ Information security policies, procedures, and regulations ☐ Specific impacts of cybersecurity gaps and breaches ☐ Monitor advancements in privacy laws and policies ☐ Privacy impact assessments ☐ Privacy disclosure statements based on laws and regulations ☐ Breach reporting	
Future Trends Affecting Key Competencies	▪ The increased reliance on virtualized and/or 'cloud-based' services will require knowledge of responsibilities of the services provider including their responsibilities for protecting sensitive data and responding/reporting potential breaches ▪ Increased use of automated tools, aided by artificial intelligence, will require understanding of how the tools will be integrated into protection of PPI within the organization and how that needs to be translated into policies, procedures and practices. ▪ Increased use of automated tools by threat actors will likely challenge existing technologies and resources intended to manage protection of PPI. Accordingly, additional tools, processes or training will be required to stay ahead of the threats. ▪ Mechanisms to support the required level of trust and organizational risk will need to be in place to support monitoring and reporting of results from automated tools. Consequently, there will be a need to	

	understand organizational risks posed to PPI/data, measures of security and what policies, processes, or procedures need to be in place. ▪ The emergence and use of quantum technologies by threat actors will fundamentally change encryption security. Encryption used to protect PPI will require knowledge and skills related to ensuring that the PPI remains protected under quantum threat.