

CAREER ROADMAP

How to Get a Privacy Job: Career Guide 2026

Learn how to begin or advance a privacy career, including common roles, transferable skills, salary evidence, certifications and career paths.

IN THIS ROADMAP

- Key takeaways
- What does a privacy professional do?
- Common privacy job titles
- Privacy career tracks
- Skills employers look for
- Privacy salary evidence

A free career roadmap from GRC Careers · AGJ, the AI governance job board

Read the latest version, and browse live privacy jobs, at ai-governance-jobs.com/ai-governance-career-guides/how-to-get-a-privacy-job

Privacy professionals help organizations use personal information lawfully, fairly and responsibly. They interpret privacy requirements, conduct assessments, manage data rights, advise product teams, respond to incidents and design programs that reduce harm while allowing useful data activity.

KEY TAKEAWAYS

- Privacy is a multidisciplinary profession that includes legal, operational, technical, governance and product roles.
- There is no single BLS occupation for privacy professionals, so salary claims should identify the underlying role or use a reputable privacy-specific survey.
- AI governance is expanding privacy work because personal data, model training, automated decisions and transparency obligations increasingly overlap.

WHAT DOES A PRIVACY PROFESSIONAL DO?

Privacy professionals turn legal and ethical expectations about personal information into business practices. They may inventory data, review products, negotiate contracts, respond to individual rights requests, manage consent, investigate incidents, conduct privacy impact assessments and report risk to leadership.

The field ranges from legal interpretation to privacy engineering. Candidates do not all need the same background.

COMMON PRIVACY JOB TITLES

1. Privacy coordinator
2. Privacy analyst
3. Data protection specialist
4. Privacy program manager
5. Privacy counsel
6. Privacy engineer
7. Product privacy manager
8. Privacy compliance manager
9. Data protection officer
10. Chief privacy officer

PRIVACY CAREER TRACKS

Track	Main focus	Useful background
Legal and regulatory	Interpreting laws, advising and contracting	Law, policy, regulatory affairs
Privacy operations	Requests, inventories, assessments and incidents	Compliance, project management, operations
Product privacy	Building privacy into products and releases	Product, legal, security, program management
Privacy engineering	Technical controls and privacy-preserving design	Software, security, data engineering
Privacy governance	Program ownership, metrics and accountability	Risk, audit, compliance, leadership

SKILLS EMPLOYERS LOOK FOR

- Privacy-law and regulatory literacy

- Data mapping and records of processing
- Privacy impact and risk assessments
- Data-subject or consumer-rights operations
- Vendor and contract review
- Incident response
- Policy and notice writing
- Product and engineering collaboration
- Data minimization, retention and access controls
- Executive communication

Privacy work requires the ability to see both the individual and the system. Strong practitioners understand what the organization wants to do with data, who may be affected and what safeguards are needed.

PRIVACY SALARY EVIDENCE

The figures below are calculated from the 22 live Privacy postings on AI-Governance-Jobs.com, of which **9** publish a salary range. This is original market data from our own board, not a survey and not an editorial estimate.

Level	Median midpoint	Middle half	Postings
Mid-level	 \$140k	\$117k – \$171k	5

Representative titles in this sample: Director, Senior Privacy Counsel, Government Information Specialist, Student Trainee, Privacy Counsel, Head of Privacy, Senior Privacy and AI Counsel, Software Engineer.

► Methodology and cautions

HOW TO GET A PRIVACY JOB

1. **Choose a track.** Decide whether your strongest route is legal, operations, product, engineering or governance.
2. **Learn the core principles.** Understand lawful use, transparency, purpose limitation, data minimization, security, individual rights and accountability.
3. **Learn the major rules for your market.** These may include U.S. state privacy laws, GDPR, HIPAA, financial privacy rules or sector-specific requirements.
4. **Build a practical portfolio.** Create a sample data map, privacy impact assessment, retention schedule, incident decision tree or product review.
5. **Translate adjacent experience.** Security, compliance, records, legal operations, research ethics and data governance all provide useful foundations.
6. **Target work with real data responsibility.** Privacy operations, vendor review, trust, risk and compliance roles can create the experience needed for advancement.

CERTIFICATIONS

The most recognizable privacy credentials come from IAPP:

- CIPP for jurisdiction-specific legal knowledge.
- CIPM for privacy program management.
- CIPT for technology-focused privacy work.
- AIGP for the growing intersection with AI governance.

Security, audit and cloud credentials may also help privacy engineers and technical privacy professionals.

PRIVACY AND AI GOVERNANCE

AI does not replace privacy as a discipline. It expands its scope. Privacy teams increasingly assess training data, automated decisions, model inputs and outputs, biometric information, transparency, vendors and individual rights in AI-enabled systems.

Professionals who can work across privacy and AI governance may have a meaningful career advantage. The IAPP survey found higher compensation among respondents working across both domains than among respondents confined to one.

SOURCES AND UPDATE NOTES

- [IAPP Salary and Jobs Report 2025–26](#)
- [IAPP Career Central](#)
- [BLS Occupational Outlook Handbook: Compliance Officers](#)
- [BLS Occupational Outlook Handbook: Information Security Analysts](#)

Internal links for publication: Privacy Jobs, Privacy Engineer Jobs, Data Protection Jobs, AI Governance Jobs, CCPA/CPRA Jobs, privacy career guides and certification comparison.

FREQUENTLY ASKED QUESTIONS

Do I need to be a lawyer to work in privacy?

No. Privacy teams include analysts, engineers, program managers, compliance professionals and operations specialists. Some counsel roles require a law license.

Is privacy a technical career?

It can be. Privacy engineering is technical, while privacy operations and legal roles may require less coding. Every track benefits from understanding how data moves through systems.

What is the best entry-level privacy role?

Privacy coordinator, privacy analyst, data-rights specialist, compliance analyst and vendor-risk roles are common entry points.

Is a CIPP certification enough to get a job?

It can strengthen a candidacy but does not replace applied experience. Employers also want evidence that a candidate can conduct assessments, manage requests or advise stakeholders.

What is the difference between privacy and data governance?

Privacy focuses on the appropriate use and protection of personal information. Data governance covers the broader ownership, quality, availability and management of organizational data.

What is the difference between a privacy officer and a data protection officer?

Titles and legal responsibilities vary. A data protection officer may have formally defined independence and duties under GDPR, while “privacy officer” is a broader organizational title.

Can cybersecurity professionals move into privacy?

Yes. Security professionals understand safeguards and incidents. They need to add legal, ethical, rights-based and product-governance perspectives.

Is privacy still growing because of AI?

AI is creating additional privacy work involving training data, automated decisions, biometrics, transparency, vendor oversight and data governance.

This roadmap is a free resource from GRC Careers.

Read the latest version, and find live privacy jobs, at ai-governance-jobs.com/ai-governance-career-guides/how-to-get-a-privacy-job · A resource from **GRC Careers**