PART OF THE AGJ PROFESSIONAL GUIDES LIBRARY

AI CAREER GUIDES / ACG-005

Chief Privacy Officer (CPO)

AI Privacy Edition

What a Chief Privacy Officer does in the age of AI, the eight core responsibilities, the skills and certifications employers want, and a 90-day plan for the first months in the seat.

Written for privacy executives, hiring managers, recruiters, and professionals moving toward privacy and AI governance leadership.

AI CAREER GUIDES / ACG-005

Chief Privacy Officer

AI Privacy Edition

Protecting people, enabling trust, and powering responsible AI through strong privacy leadership.

THE 8 CORE RESPONSIBILITIES

- 01 Privacy strategy & policy
- 02 Data protection & compliance
- 03 Privacy by design & default
- 04 Data minimization
- 05 Cross-border data governance
- 06 AI privacy risk oversight
- 07 Trust & transparency
- 08 Incident response

THE LAWS THEY ANSWER TO

GDPR | CCPA | CPRA | LGPD | PIPEDA | EU AI Act

CERTIFICATIONS THAT SIGNAL THE WORK

CIPP | CIPM | AIGP | CDPSE

YOUR FIRST 90 DAYS

Days 1-30
Find out what you have. Get the AI inventory and data map. Learn where personal data enters and who is pointing AI at it.

Days 30-60
Rank the risk. Score AI systems by data sensitivity and the cost of a wrong decision. Fix the loudest gap first.

Days 60-90
Make it repeatable. Put privacy review into product intake. Give the board one page and three metrics you report every quarter.

The Chief Privacy Officer career guide at a glance · Source: GRC Careers

AI runs on personal data, and personal data comes with rules. As companies push AI into hiring, lending, healthcare, insurance, and customer service, the hard question stops being what the model can do and becomes whether the company is allowed to use people's information that way. Answering that question is now the Chief Privacy Officer's job.

The modern CPO owns privacy strategy and data protection across the business: keeping the company on the right side of the law, deciding what data AI systems are allowed to touch, and holding the trust of customers, employees, and regulators while the technology moves fast. Get privacy right and AI adoption speeds up because people believe you. Get it wrong and one bad automated decision becomes a headline.

Why the CPO Matters

The Chief Privacy Officer sits where law, technology, ethics, and business strategy meet. Eight core responsibilities define the role in AI governance:

- **Privacy strategy and policy.** Set enterprise privacy strategy, policy, and standards, and make sure they line up with business goals and AI plans instead of fighting them.
- **Data protection and regulatory compliance.** Keep the company compliant with global privacy law, including GDPR, CCPA, CPRA, LGPD, PIPEDA, and the privacy-facing parts of the EU AI Act.
- **Privacy by design and by default.** Build privacy into products, services, and AI systems from the first design meeting, not as a fix after launch.
- **Data minimization and purpose limitation.** Push the company to collect and keep only the personal data it actually needs, for a purpose it can defend.
- **Cross-border data governance.** Manage international data transfers, localization rules, and the jurisdiction-by-jurisdiction obligations that follow the data.
- **Privacy risk assessment and AI oversight.** Review AI systems for privacy risk before they ship and keep watching them for the life of the system.
- **Stakeholder trust and transparency.** Explain plainly how the company uses data, to customers, employees, partners, regulators, and the board.

- **Incident response and continuous improvement.** Own the plan for when something goes wrong, and tighten the program as laws and technology change.

The Connection Between Privacy and AI Governance

AI sharpens old privacy questions and adds new ones. The CPO is the person who has to answer them:

- What personal data trained this model, and what data feeds it now?
- Was that data collected for this purpose, and is using it this way lawful?
- Can a person find out an automated decision was made about them, and challenge it?
- Are we minimizing data, or hoarding more than the job requires?
- Where does the data physically live, and which borders does it cross?
- When something breaks, how fast can we detect it, contain it, and tell the people affected?

Answering those well protects people, lowers regulatory exposure, and earns the trust that AI adoption quietly depends on.

Skills Employers Are Looking For

As companies expand what AI does, they look for privacy leaders who can show real experience in:

- Privacy program management
- Global privacy law and regulation
- Privacy by design
- Data protection impact assessments
- AI governance and oversight
- Data minimization and governance
- Incident and breach response
- Cross-functional leadership
- Executive and board communication
- Change management

Technical knowledge alone does not carry the role. The CPOs who get hired can take a dense legal obligation and turn it into a decision an engineer, a regulator, and a customer can all live with.

Recommended Certifications

No certificate is strictly required to be a CPO, but a few signal you can do the work. The common ones come from the IAPP:

- **CIPP** for privacy law by jurisdiction (CIPP/US, CIPP/E for Europe).
- **CIPM** for building and running a privacy program day to day.
- **AIGP**, the AI Governance Professional credential, for the AI-specific oversight the role now carries.
- **CDPSE** from ISACA for the privacy-engineering and technical side.

For a credential-by-credential breakdown of what each covers, what it costs, and who it is for, see the certification guides at **GRC-Careers.org**.

CURRENT CPO OPPORTUNITIES

See current Chief Privacy Officer and privacy leadership roles on AI Governance Jobs.

Browse Chief Privacy Officer jobs →

Your First 90 Days as a Chief Privacy Officer

A new CPO rarely fails on legal knowledge. They fail by not knowing what the company actually holds and does with data. The first quarter is about fixing that blind spot.

Days 1 to 30: find out what you have

Get the AI inventory and the data map, or start building them if they do not exist. Sit down with legal, security, and every product team already shipping AI features. Read the last two years of privacy complaints, data subject requests, and any letters from regulators. You are answering one question: where does personal data enter this company, and who is already pointing AI at it?

Days 30 to 60: rank the risk

Score AI systems by two things: how sensitive the data is, and how much a wrong decision costs a real person. Stand up a data protection impact assessment process, or fix the one

you inherited, so no high-risk AI ships without one. Then fix the loudest gap first. It is usually a system making decisions about people with no human in the loop.

Days 60 to 90: make it repeatable

Put privacy review into the product intake process so it is a default step, not a favor someone remembers to ask for. Give the board a single page: what data the company holds, where the AI risk concentrates, and what you are doing about it. Agree on three metrics you will report every quarter, and report them.

Frequently Asked Questions

What does a Chief Privacy Officer do?

A CPO owns how an organization collects, uses, and protects personal data. Day to day that means setting privacy policy, keeping the company compliant with laws like GDPR and CCPA, reviewing new products and AI systems before they launch, and being the person who answers to regulators when something goes wrong.

What is the difference between a CPO and a Data Protection Officer?

A Data Protection Officer is a specific role required by GDPR, and the law says it has to stay independent, even to the point of reporting its own employer to regulators. A Chief Privacy Officer is a business executive who owns privacy strategy for the whole organization. Some companies have both, with the DPO reporting into the CPO. The CPO sets direction; the DPO is a legally mandated watchdog.

What certifications help you become a CPO?

The IAPP credentials are the usual ones: CIPP for privacy law, CIPM for running a privacy program, and AIGP for AI governance. ISACA's CDPSE covers the technical, privacy-engineering side. None are strictly required, but together they show an employer you can do the work.

How is AI changing the Chief Privacy Officer role?

AI moved privacy from a paperwork function to a decision-making one. CPOs now review training data, automated decisions, and how models behave, not just cookie banners and consent forms. The EU AI Act ties privacy and AI oversight together, so in many companies the CPO now owns both.

What background do most CPOs come from?

Usually privacy or data protection law, compliance, or information security. The common thread is someone who can read a regulation, understand a technical system, and translate between the lawyers, the engineers, and the executives without losing any of them.

Final Thoughts

The Chief Privacy Officer is turning into one of the most important executives in AI governance. By protecting people, building privacy into how AI gets made and used, and speaking plainly to regulators and the public, a strong CPO turns privacy from a cost center into a reason customers trust the company. The organizations that take privacy leadership seriously will be the ones able to build AI that is lawful, transparent, and worth trusting.

WHO SHOULD READ THIS GUIDE

- Chief Privacy Officers
- Data protection officers
- Privacy program leaders
- Privacy counsel
- Compliance and risk executives
- Security and data leaders
- Executive recruiters
- Professionals pursuing AI governance leadership

Related AI Governance Essentials

Chief Privacy Officers should also know these foundational governance topics:

- What Is an AI Inventory?
- What Is an AI Use Policy?
- How to Conduct an AI Risk Assessment
- Browse the full AI Governance Essentials series →

Related AI Career Guides

- Chief Information Security Officer: AI Security Edition
- Chief Compliance Officer: AI Compliance Edition

- Chief Risk Officer: AI Risk Edition
- Chief Data Officer: Data Leadership Edition
- Chief Audit Executive: AI Audit Edition
- AI Governance Manager
- Browse all AI Career Guides →

ABOUT THE AI CAREER GUIDES SERIES

The AI Career Guides (ACG) series looks at how AI is reshaping executive leadership across governance, risk, compliance, cybersecurity, audit, privacy, data, and technology. Each guide pairs practical career insight with the AI governance resources that back it up.
