

A Path to a Career in Privacy and AI Governance



Table of Contents

1.0 Introduction	1
2.0 What Does It Mean to Have a Career In Privacy?	2
2.1 What Does a Privacy or AI Governance Professional Do?	3
2.2 Information Privacy and Information Security: What's The Difference?	5
3.0 Why Become a Privacy and AI Governance Professional?	6
3.1 The Benefits of Joining The Profession	6
4.0 Where Do You Fit In?	8
5.0 What Education Do I Need?	10
6.0 The Role of a Certification	11
6.1 What is the IAPP?	11
6.2 Which Certification Fits You?	12
6.3 Do I Need a Technical Background?	14
6.4 Other Certifying Bodies Worth Knowing	15
7.0 How Do I Gain Experience?	17
7.1 Making the Transition	17
7.2 Write	18
7.3 Speak	19
7.4 Network	19
7.5 Take CLEs and Continuing Education	20
7.6 Make It Count	21
7.7 Build Your People Skills	22
8.0 Landing Your First (Or Next) Job in Privacy	23
8.1 What Do Employers Actually Want To See?	23
8.2 Where Do I Find Jobs?	23
8.3 Fellowships and Internships Worth Knowing About	24
9.0 There is No Single Path	25
10.0 Resources for Building a Career in Privacy and AI Governance	27

SECTION 1

Introduction

This guide is organized as a practical path: first, it explains what privacy and AI governance work looks like; then it helps you assess which background you are coming from; and finally, it points you toward education, certifications, experience-building, and job-search strategies.

Privacy is one of the youngest professions in the modern job market and one of the fastest-changing. A decade ago, “privacy professional” wasn’t a job title that most companies had, let alone a career path that someone could plan for. Today, it’s a growing, well-paying field, with its own certifications, professional associations, and a clear—if still in the making—idea of what the job really entails.

That growth didn’t happen in a vacuum. The European Union’s General Data Protection Regulation (GDPR) rollout in 2018 turned privacy into a legal requirement with real financial teeth across not only Europe but globally; the California Consumer Privacy Act (CCPA) and California Privacy Rights Act (CPRA), followed by a wave of comprehensive privacy laws in other U.S. states, did the same in the United States; and, more recently, the E.U.’s AI Act has begun doing for AI governance what the GDPR did for privacy roughly a decade ago. Each new law creates positions that didn’t exist before, which is a large part of why the field keeps expanding rather than settling into a fixed shape.

That is both the opportunity and the challenge. Because the profession is still young, there is no single, well-trodden path into it. While many privacy professionals come from a legal background, there is no equivalent of going to law school and passing the bar exam. People enter privacy from a range of backgrounds, including IT, compliance, product management, and sometimes fields that have little obvious connection to data. And because the field continues to evolve, especially with the rise of AI governance, even people already working in privacy are often building their careers as they go.

This guide is meant to be a starting point for anyone who is curious about this field. It covers what privacy really is, what day-to-day work looks like, why people are attracted to it, how to get in with no prior experience, what role certifications play, and how to think about landing your first or next position.

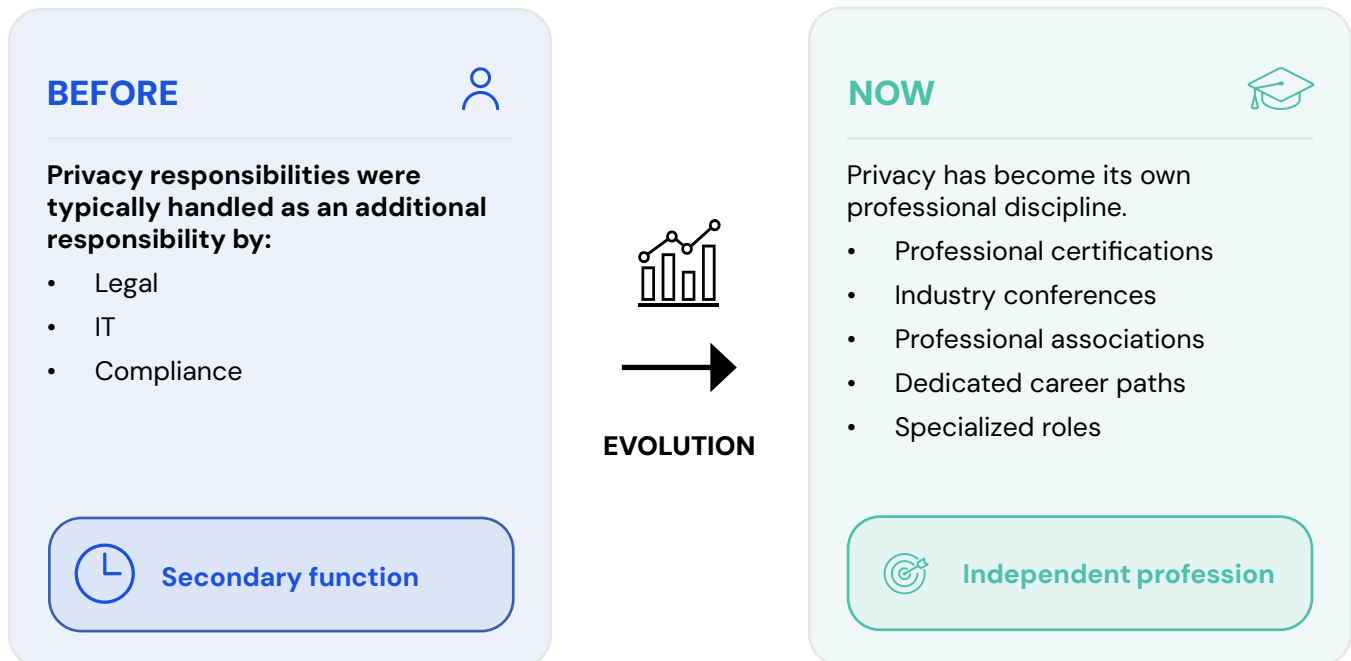
Along the way, we’ll be upfront about the parts that are genuinely difficult, because this is meant to be a realistic guide, not a sales pitch.

Wherever you start, our goal is simple: by the end of this guide, you should have a clear and honest picture of what a career in privacy looks like, and a real idea of whether, and how, it fits you.

SECTION 2

What Does It Mean to Have a Career In Privacy?

Having a career in privacy means being part of a rapidly growing professional identity. In the last decade, privacy has gone from being a secondary responsibility that someone in the legal or IT department took on in addition to their actual work, to being a discipline recognized in its own right. The field now has its own certifications, its own conferences, and its own professional associations. Some organizations even have a department dedicated entirely to privacy issues, much like a human resources, information security, or marketing department.



That evolution is accelerating thanks to the emergence of big data, data mining, and artificial intelligence (AI). Questions that didn't exist five years ago, such as how to govern the use of personal data by an AI system, are now central to the work. That means privacy professionals today don't just apply a consolidated body of knowledge—in many cases, they're helping to build it.

2.1 | What Does a Privacy or AI Governance Professional Do?

At its core, the goal of the profession is simple to articulate, even if the job itself isn't: to protect personal data and make sure organizations handle it responsibly.

In practice, that goal is divided into several different components. There is the legal side, which involves understanding what the law requires. There's the operational/governance side, building the day-to-day processes that keep an organization in compliance. There's also a commercial side, negotiating data processing agreements, vendor contracts, and other terms that govern how personal data moves between organizations. And there's the technical side, embedding privacy directly into the products and systems that collect and use data in the first place.



Legal

Understand what the law requires.



Operational

Build the daily compliance processes.



Commercial

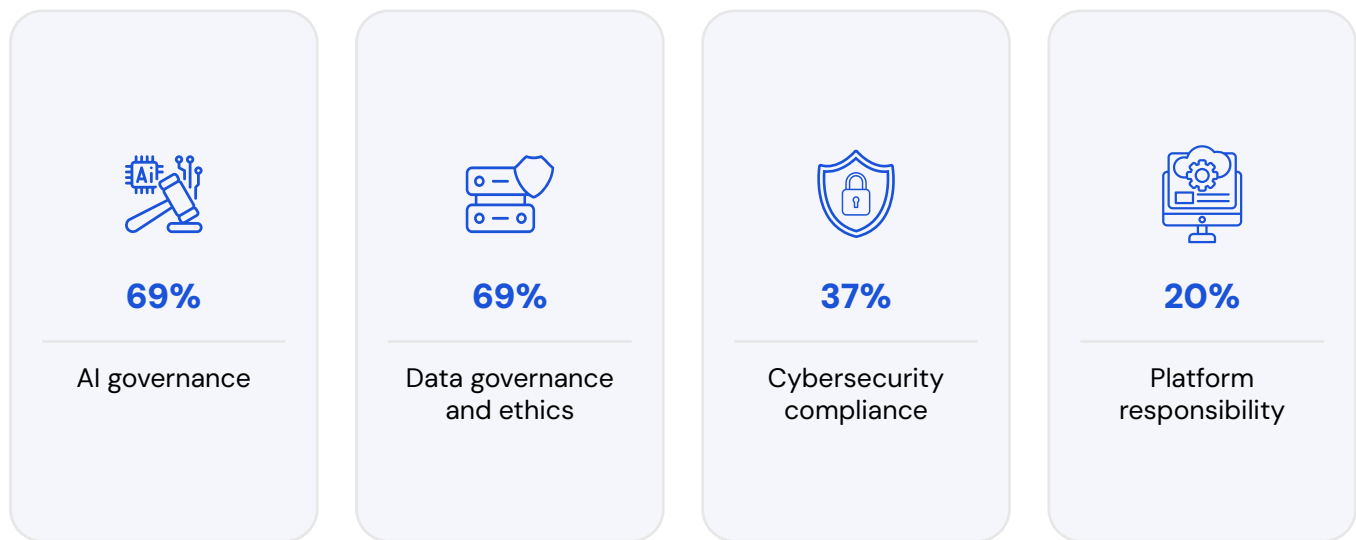
Negotiate the contracts that move data between organizations.



Technical

Integrate privacy into products and systems.

What makes this profession interesting now is how quickly that scope is expanding. According to IAPP's 2024 Privacy Governance Report, most privacy teams have been asked to take on responsibilities far beyond their original job description. Among the Chief Privacy Officers surveyed, 69% have taken additional responsibility for AI governance, 69% for data governance and ethics, 37% for cybersecurity compliance, and 20% for platform responsibility. More than 80% of privacy teams overall report taking on responsibilities that go beyond privacy in the traditional sense.¹



That growth is precisely where the figure of the AI governance professional comes in. Like a privacy professional, this specialist focuses on AI systems and ensures that the way an organization develops, implements, and monitors AI tools is secure, fair, and compliant. In practice, the two roles constantly overlap. Most people working in AI governance today come from a privacy background, and most organizations treat AI governance as an extension of their existing privacy program, rather than something built from scratch.

In other words, if you ask what a privacy or AI governance professional actually does on a day-to-day basis, the honest answer is that it depends on the organization. It is also changing rapidly. A privacy analyst in a company can spend most of their time on compliance documentation. In another, they might primarily be responsible for responding to data subject access requests (i.e., requests of individuals to access the data the company holds on them). In yet another, they might be deeply involved in AI risk assessments, vendor reviews, or even cybersecurity issues that weren't previously part of the privacy realm.

None of this happens in isolation. A privacy or AI governance professional spends as much time in Legal, Engineering, Marketing, and HR meetings as at their own desk, and the job only works if

Note: Percentages reflect multiple-response survey data (respondents could select more than one area)

¹ IAPP, Privacy Governance Report 2024 (Nov. 2024), <https://iapp.org/resources/article/privacy-governance-report/>

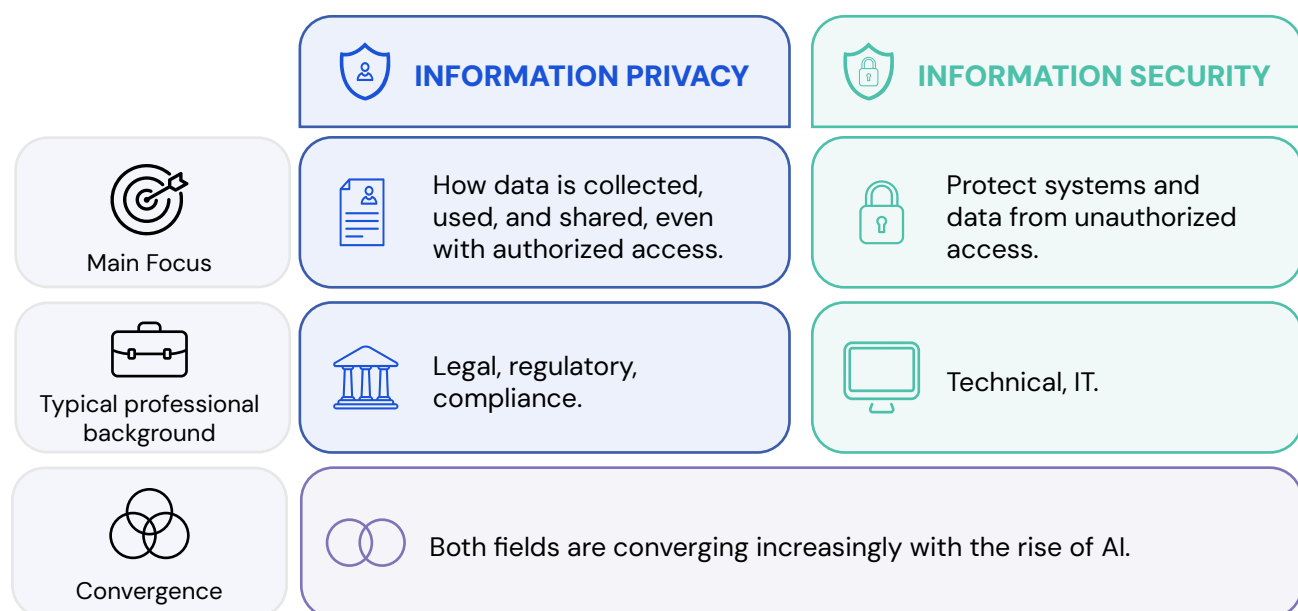
those teams trust them enough to ask before—not after—they launch something. Being technically right means little if no one comes to you early enough to act on it. That’s why the strongest people in this field build relationships across the organization deliberately, because the end goal isn’t a privacy department that catches problems, it’s a company where privacy is understood as everyone’s job.

2.2 | Information Privacy and Information Security: What’s The Difference?

A common point of confusion worth clarifying is that information privacy and information security are related, but they are not the same thing. This can be particularly confusing because in many places across the globe—most prominently, in Europe—the term “data protection” is used synonymously with information privacy. “Protecting” data conjures up images of would-be hackers, malware, and other security threats.

Information security is in the realm of cybersecurity experts, and it is primarily focused on protecting systems and data from unauthorized access. Privacy, on the other hand, deals with how personal data is collected, used, and shared, even when that access is fully authorized.

This difference is also reflected in the professional profiles. Many people come to cybersecurity from technical and IT fields, while those who work in privacy often come from legal, regulatory, or compliance fields. Although both fields are increasingly converging, especially as AI systems pose challenges that affect both security and the processing of personal data, they remain disciplines with distinct goals and approaches.



SECTION 3

Why Become a Privacy and AI Governance Professional?

There are compelling, concrete reasons to choose this field deliberately, not just fall into it: strong pay and interesting work that rarely stays the same for long. But the honest answer is that people arrive at those reasons differently. Some fall into it by accident, moving from a position in law, IT, or compliance where questions about privacy or AI kept popping up until it became their primary job. Others choose it on purpose, because they want to work at the center of one of today's biggest technological changes: how personal data and AI systems are governed.

Whatever the path, it's worth honestly asking why anyone would choose this field over another. Privacy isn't the only growing realm in technology or law, and it's not the easiest field to break into. The rest of this section makes the case for why it's worth the effort anyway.

3.1 | The Benefits of Joining The Profession

Ask enough people why they stayed in privacy, and the same two reasons keep surfacing: pay and pace. What's worth exploring is not just that these reasons exist, but why each one holds up as well as it does on closer look.

Let's start with pay. According to IAPP's 2025–26 Salary and Jobs Report, the largest and most globally diverse salary survey the organization has conducted, the global average total compensation in privacy, AI governance, and digital responsibility roles now stands at \$200,000. Looking specifically at how domain focus affects pay, professionals who manage both privacy and AI governance have a median total compensation of more than \$169,700, compared to \$123,000 for those focused solely on privacy and \$151,800 for those focused solely on AI governance. In other words, combining both domains is associated with a meaningfully higher median salary than specializing in just one.

GLOBAL AVERAGE (ALL ROLES, ALL SENIORITY LEVELS)

\$200,000 MEANGlobal average total compensation
Pulled upward by senior, executive & technical roles

MEDIAN, BY DOMAIN FOCUS

\$169,700 MEDIAN

Privacy + AI governance combo

\$151,800 MEDIAN

AI governance only

\$123,000 MEDIAN

Privacy only

Certifications matter, too, at least when it comes to salary. Multiple IAPP certifications—and especially the Fellow of Information Privacy (FIP) designation (a status earned by holding two IAPP certifications plus at least three years of privacy experience, rather than a separate exam)—are associated with higher salaries, and the vast majority of those in the industry have at least one.

But the honest reason why many people stay in privacy is less for the salary and more for the pace. This is a field where rules are still being drafted. AI governance, in particular, barely existed as a job category a few years ago, and is now at the center of the profession's growth. For those who want a job that keeps changing and growing, rather than a role they can learn once and then repeat for years, that's a real draw, not just a marketing line.

None of this means that the sector is easy to enter, nor that a high salary is guaranteed from day one. In the next section we will walk through the realistic path. But if you ask if privacy is a field worth entering, the numbers say yes, and they say so more clearly than they did even a year ago.

SECTION 4

Where Do You Fit In?

You don't need a law degree. You don't need to know how to code. And you certainly don't even need to know what a privacy impact assessment looks like yet.

If you're starting without any prior knowledge, start here. This is more common than one would expect. Privacy is one of the few fields that are actively designed for career changers, and most people working in it today also started elsewhere. There is no single and adequate resume to enter.

What you need is an honest answer: do any of the paths below sound familiar?

If you're coming from the legal field: you know how to read a regulation. What's new is specificity. Privacy law is advancing faster and spanning more sectors than almost any other legal specialty currently, making it one of the most future-proof directions a legal career can take.



To highlight this fact, the American Bar Association now lists "Privacy Law" as one of just nineteen specialties it recognizes. To date, 37 States in the U.S. allow practicing attorneys to identify themselves as a "specialist" in privacy law. In order to qualify, many states require passing at least two IAPP certification exams.

► To learn more, you can read our article: ["Privacy Law Certification: The PLS Designation"](#).

If you're coming from a compliance or risk background: you know what it's like to translate regulation into action. That instinct for processes, documentation, and accountability is precisely what privacy program management is based on, managing the day-to-day of how an organization actually protects data, not just knowing the theory behind it.

If you're coming from IT or engineering: you've spent years thinking about systems, data flows, architecture, and access controls. That instinct doesn't disappear in privacy. It becomes your edge. People with your expertise often move into technical privacy roles, those who not only interpret the law, but integrate it directly into how products and systems work.

If you're coming from marketing or product: this topic surprises people, but marketing or product teams are often the first to feel the weight of privacy regulation, cookie consent, data collection, and AI-powered personalization. If you've ever had to explain to the legal department why a campaign needed to change, you already understand more about this field than you think.

If you're coming from HR: you already manage some of the most sensitive personal data an organization has: employee records, performance reviews, monitoring tools, benefits information. As companies adopt AI for recruitment, performance management, and workforce analytics, HR professionals who understand privacy are becoming increasingly valuable, because both the human and process sides are already understood.



Legal

You know how to read a regulation.



Compliance

You know how to turn regulation into action.



IT

You understand systems and data flows.



Marketing

You already navigate privacy in campaigns and products.



HR

You already manage sensitive personal data.

SECTION 5

What Education Do I Need?

It helps to be clear about something the field doesn't always say out loud: not all directions require the same starting point when it comes to education. Take degrees as an example. Like nearly all professions in a modern corporate environment, getting into privacy will likely require a four-year college degree, but rarely a specific one. Employers are not scanning resumes for a privacy major, because it barely exists yet. What they're looking for is the baseline: critical thinking, writing ability, and the discipline to work through dense material, which is most of what the job actually involves day in and day out. More specialized areas within the field, such as advising on legal issues, call for advanced degrees on top of that, since interpreting and applying regulation is, at its core, legal work.

A degree alone doesn't cover everything the job asks of you. Non-formal, hands-on technical literacy matters just as much, and it's the part that catches people off guard. You can't properly advise on cookie compliance if you don't know what a cookie actually does. You can't govern AI systems if you don't understand, at least at a basic level, how machine learning models are trained on data. This doesn't mean you need to learn to code. It means you need to be curious enough to understand the systems you're advising on, not just the regulations that apply to them. We'll come back to this question—i.e., how much technical knowledge you actually need—later in this guide, because the real answer depends heavily on which path you take.

A handful of colleges have started offering programs built specifically for privacy, a sign of how quickly the field is professionalizing. Carnegie Mellon, for example, offers a Master of Science in Information Technology – Privacy Engineering (MSIT-PE), one of the only technical privacy-focused graduate programs in the country, and a strong option if your path is leaning technical from the start². Other schools take a different approach, offering executive certificate programs instead of full degrees, aimed at working professionals rather than full-time students. Harvard Online's *Data Privacy and Technology*³ course and Cornell's eCornell *Data Security and Privacy Policy* certificate⁴ both offer standalone privacy credentials you can complete alongside a job, without pausing your career to go back to school. None of this means a specific privacy degree is required to break into the field. It isn't, and plenty of people in the field don't have one. But the growth of programs like these is a sign of how established the field has become, and how seriously employers now take formal privacy education.

Education gives you the foundation, but it's rarely the finish line. Once you have that baseline in place, whether it's a general degree, hands-on technical literacy, or one of the specialized programs above, the next natural step is proving what you know in a way employers recognize. That's where certification comes in.

² Carnegie Mellon University. (n.d.). Master of Science in Information Technology – Privacy Engineering (MSIT-PE). Carnegie Mellon University. <https://privacy.cs.cmu.edu/masters/index.html>

³ Harvard Online. (n.d.). Data Privacy and Technology. Harvard University. <https://harvardonline.harvard.edu/course/data-privacy-technology>

⁴ Cornell University. (n.d.). Data Security and Privacy Policy Certificate. eCornell. <https://ecornell.cornell.edu/certificates/financial-management/data-security-and-privacy-policy/>

SECTION 6

The Role of a Certification

Do you need a certification to work in privacy? The short answer is no. Many successful privacy professionals built their careers before they earned one, and hands-on experience will always carry real weight for employers.

Certifications aren't the only way into privacy, but they're the fastest way to prove you belong in the room, especially if you're coming from outside the field and don't have years of job titles to point to instead.

With increasing frequency, privacy certifications are included on job posting requirements. This is, in part, a result of the fact that hiring teams like having objective criteria to point to when making decisions. And this is especially true in new or emerging fields, like privacy, where the experience and background of applicants can vary widely. Certification provides a marker that is easily pointed to—and easily filtered for.

6.1 | What is the IAPP?

The IAPP (recently rebranded from its former name, the International Association of Privacy Professionals) is the largest professional organization in the field, and its certifications have become the closest thing to an industry standard that privacy has. These include the Certified Information Privacy Professional (CIPP), Certified Information Privacy Manager (CIPM), Certified Information Privacy Technologist (CIPT), and Artificial Intelligence Governance Professional (AIGP) designations.

All IAPP certifications are accredited by the ANSI National Accreditation Board under ISO/IEC 17024, which is a formal way of saying that employers, regulators, and other certifying bodies recognize them as legitimate, not just as a badge from an online course. Beyond the exams themselves, IAPP also runs KnowledgeNet chapters in more than 160 locations worldwide, conferences, and a job board, which makes it as much a professional community as a certifying body.

Getting IAPP certified is associated with real, measurable benefits. According to IAPP's own 2025–26 Salary and Jobs Report, professionals who hold multiple certifications, and especially those who earn the Fellow of Information Privacy (FIP) designation, report higher salaries than peers without them. Unlike the CIPP, CIPM, CIPT, and AIGP, the FIP isn't a fifth certification with its own exam. It's a status you become eligible for once you hold two of those certifications and have at least three years of privacy experience, with three peer references. Equally important, certifications give you a specific, searchable credential to put on a resume or LinkedIn profile, which matters more than it sounds like it should, since many recruiters filter candidates by the exact name of a certification—not by general keywords like "privacy experience."



Certification isn't free, and it's worth budgeting for before you commit. A first IAPP exam costs \$550, discounted to \$375 for each certification after your first; the newer AIGP exam runs higher, at \$649 for members or \$799 for non-members. On top of the exam itself, maintaining a certification requires either an annual IAPP membership (\$50 to \$295, depending on your employment status) or a standalone \$250 maintenance fee every two years, plus 20 continuing privacy education credits bi-annually. None of this counts training materials or a prep course, which most candidates find worth adding given how broad the exams are.

► For the full breakdown by certification, see our article: [“What Are the Costs of IAPP Certification?”](#)

6.2 | Which Certification Fits You?

Here's what each path really teaches you, and where it usually takes you.

Law and Regulation (CIPP)

You can build a deep understanding of what's regulated, what's required, and what's really at risk, the kind of knowledge that almost any other privacy position assumes you already have. This is usually where a career in privacy begins, whether you come from legal, compliance, or start from scratch with no experience at all. This is the knowledge base that covers the CIPP, available in the U.S., Europe, and Canada versions. There are also jurisdiction-specific CIPP exams for China, Brazil, Asia (covering Singapore, Hong Kong, and India), and Australia, though these exams have not yet fully established themselves as industry standards. Remember, this path builds your privacy-specific knowledge, but if your goal is to specifically practice privacy law, it goes alongside a law degree, not instead of one. This path tends to energize people who are comfortable making a defensible call without a perfect answer in the regulation, and who enjoy writing that has to hold up to scrutiny. It tends to wear out people who are hoping for clear, black-and-white rules, since privacy law rarely offers those.

Running Programs (CIPM)

You can learn how privacy is actually operationalized within an organization: the policies, vendor management, incident response, the day-to-day machinery behind compliance. It's what makes you the person a company trusts to truly manage privacy, not just understand it. This is the knowledge base that covers the CIPM, a natural next step if you are already in compliance or in risk management. This path tends to energize people who take real satisfaction in order, process, and follow-through, the kind of person who can look at a requirement and immediately see the workflow that will make it stick. It tends to wear out people who expected mostly strategic work and found themselves managing a backlog instead.

Technical (CIPT)

You can learn how to integrate privacy directly into products and systems, rather than explaining it later: privacy engineering, data life cycle, and privacy-enhancing technologies. In this sector, IT and engineering profiles are usually the fastest to learn it. This is the knowledge base that the CIPT covers. As stated, this certification deepens technical knowledge about privacy; it does not teach general programming skills from scratch. This path tends to energize people who like translating between two worlds, explaining engineering realities to legal and compliance teams and vice versa. It tends to wear out people who want to stay purely on one side of that conversation, either fully technical or fully removed from the systems themselves.

AI Governance (AIGP)

You can build an understanding of the risk structures and governance specific to AI systems, a space in which regulation is still catching up. It's worth exploring if you already work near AI systems, or want to get ahead of a space that's about to become much more saturated. This is the knowledge base that AIGP covers. This path tends to energize people who are comfortable shaping expectations before the rules are fully settled. It tends to wear out people who prefer working from an established playbook, since AI governance is still being written in real time.

Certification Comparison By Career Path

Certification	Best Fit	What It Signals	Good First Step
 CIPP	Law and regulation	Understanding privacy laws, regulatory requirements, and legal risk.	Start if you want a strong foundation in privacy rules and terminology.
 CIPM	Program management	Ability to turn requirements into policies, processes, and accountable workflows.	Choose this if you already work in compliance, risk, operations, or governance.
 CIPT	Technical privacy	Fluency in privacy by design, data life cycle, and product or systems privacy.	Explore this if your background is IT, engineering, product, or security-adjacent.
 AIGP	AI governance	Understanding of AI risk, governance frameworks, and responsible AI oversight.	Consider this if your work already touches AI tools, models, or automated decision-making.

👉 **Still curious about which of these suits you best?** Our [5-minute quiz](#) can help you clarify this, but the descriptions above are a good starting point on their own.

6.3 | Do I Need a Technical Background?

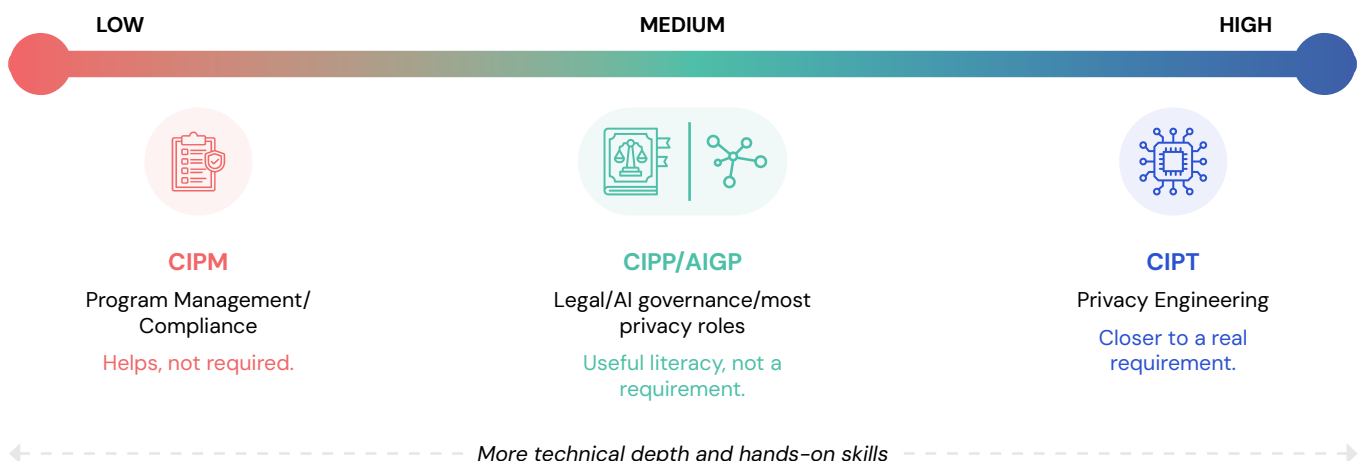
The short answer: it helps, but it's not required, especially early in your career or if you're transitioning from a non-technical field. This is one of the most common concerns people have before entering privacy, so it's worth taking it seriously rather than quickly dismissing it with a "don't worry about it."

Here is what actually helps, without needing to become an engineer. A functional, high-level understanding of how data moves through a system, what a database is, what an API does, and what a data flow diagram shows, makes you more effective in almost any privacy role. This is true even in roles that are mostly legal or operational. It helps you ask sharper questions in a meeting with engineers, understand what they mean when they describe a system, and spot a risk that a purely legal reading of a regulation might miss entirely. None of this requires being able to build the system yourself. It requires being able to follow along and ask good questions.

That said, it's worth being honest about where the line actually sits. You don't need to code to build a career in program management, compliance, or most AI governance roles, and plenty of people spend an entire career in privacy without ever opening a code editor. Technical depth becomes closer to a real requirement only on the privacy engineering path specifically, where the job itself involves building privacy directly into products and systems.

If you're early in your career, or transitioning in from a non-technical field, and you want to build this kind of literacy without committing to a coding bootcamp, consider a few low-lift options: free introductory courses on how databases and APIs work, shadowing your organization's engineering team during a data mapping exercise, or simply asking an engineer on your team to walk you through how user data flows through one product you both work on. None of these make you a technical expert. They make you fluent enough to be useful in a room full of people who are.

How much technical background do you need for each certification path?



6.4 | Other Certifying Bodies Worth Knowing

IAPP is not the only organization in this space, and depending on your background, one of these may fit your path better.

ISACA, best known for its security certifications like CISA and CISM, offers the CDPSE, Certified Data Privacy Solutions Engineer. It is an experience-based, technical certification, the first of its kind, built specifically for professionals implementing privacy by design directly into systems, networks, and products. It covers three domains: privacy governance, privacy architecture, and data life cycle, and it sits closer to the technical path than CIPP or CIPM do. To fully certify, you need at least three years of relevant experience in data privacy governance, privacy architecture, or data life cycle work, though you're allowed to sit the exam before meeting that requirement, and only need to submit proof of experience afterward. Because ISACA already has strong name recognition among security teams, CDPSE tends to be the more natural next step if you're coming from IT, engineering, or a cybersecurity background specifically, rather than from law or compliance.

ISACA also offers the Advanced in AI Audit (AAIA) certification, aimed at experienced auditors who want to validate AI governance, risk, and audit skills specifically. It requires an existing credential like the CISA as a prerequisite, so it tends to suit professionals coming from an audit background rather than someone starting from zero.

For a different angle entirely, PECB offers the ISO/IEC 42001 Lead Implementer certification, tied directly to the international standard for AI management systems rather than to a single professional body. It's a strong fit if your work leans toward helping organizations actually build and operate an AI governance program, not just advise on it, and it pairs naturally with a compliance or program management background.⁵

ISC2, the organization behind the well-known CISSP, offers certifications like the CGRC (Governance, Risk and Compliance), which touch privacy-adjacent work without being privacy-specific certifications on their own. These tend to make the most sense if your path runs through security first, and privacy is one part of a broader governance, risk, and compliance role rather than the center of your job.

Both ISACA and ISC2 certifications require ongoing continuing education to maintain, similar to IAPP. None of these bodies compete directly with IAPP so much as serve different starting points.

If your path runs through law, program management, or AI governance specifically, IAPP is still the clearest place to start. If your path runs through the technical side of privacy engineering and you're already comfortable in security-adjacent work, CDPSE is worth exploring alongside, or instead of, CIPT, depending on how much hands-on system experience you already have.

⁵ PECB. (n.d.). *ISO/IEC 42001 Lead Implementer*. [PECB. ISO/IEC 42001 Lead Implementer Certification](#)

				
Certification key	CIPP, CIPM, CIPT, AIGP	CDPSE	CGRC	ISO/IEC 42001 Lead Implementer
Best for	Legal, program management, AI governance	IT, engineering, cybersecurity	Security-first roles where privacy is part of a broader GRC function	Compliance or program management professionals building and operating AI governance programs
Type of profile	Privacy generalist	Technical, experience-based (3+ years)	Governance, risk & compliance	AI management system implementer

SECTION 7

How Do I Gain Experience?

Certifications show that you understand the theory. What they don't do is show that you can apply it, and that gap is exactly what employers try to fill when they look at a candidate's track record. The good news is that building real, visible privacy expertise doesn't first require a professional title in privacy. There are several ways to get started before you have one.

7.1 | Making the Transition

Moving into privacy from another field is rarely a simple leap. It's usually a series of small, deliberate moves that bring your day-to-day work closer to privacy, even before your title changes. The most practical way to do this is to look for privacy-related work within the position you already have.

Below are some examples of what this might look like in practice.

- **If you're an employment attorney:** Look for opportunities to work on issues related to the use of AI in hiring and interviewing, an area where employment law and AI governance increasingly overlap.
- **If you're in compliance or risk:** Volunteer to handle your team's next vendor privacy review, or the next data processing agreement that comes to your desk. This is exactly the muscle privacy program management is based around.
- **If you're in IT or engineering:** Raise your hand to be the point of contact in your team's next data mapping or privacy impact assessment exercise. It puts you directly into the process instead of hearing about it secondhand.
- **If you're in marketing or product:** Volunteer for the next project that deals with cookie consent, data collection design, or AI-powered personalization. These are the moments when legal and privacy teams end up getting involved anyway, so you're already halfway there.
- **If you're in HR:** Volunteer to review the privacy implications of a new recruitment tool, employee monitoring system, or workforce analytics platform your company is adopting. AI is rapidly appearing in HR technology, and organizations increasingly need someone who understands both the employment side and the privacy side of that change.
- **If you don't have privacy-adjacent work available yet:** Ask to shadow or sit in on a meeting where privacy or AI governance issues come up, even as a silent observer. Most privacy teams are understaffed and open to it, and it costs your manager nothing to say yes.



Employment Attorney

Look for AI issues in hiring.



Compliance/Risk

Volunteer for the next vendor privacy review.



IT/Engineering

Raise your hand for the next data mapping exercise.



Marketing/Product

Volunteer for cookie consent or AI personalization projects.



HR

Review the privacy implications of a new HR tool.



No privacy-adjacent work yet

Ask to sit in on a privacy meeting.

As these examples show, there is no standardized, well-trodden path. Breaking into a new and emerging career field sometimes requires creativity.

And none of these examples represent a complete career change. They're small, visible ways to start doing pieces of the work before you have the title. Over time, they add up to a body of work that you can point to: a project, a process you helped build, or a review you led. That body of work becomes the bridge between your current title and the one you actually want.

One last thing worth remembering: very few privacy professionals planned this career from the beginning. Most arrived here gradually, building on experience in law, IT, compliance, product, human resources, or something else entirely. Your transition doesn't have to happen all at once, or follow anyone else's timeline.

7.2 | Write

Privacy is a field that rewards public thought. A short article breaking down a new regulation, a LinkedIn post analyzing a recent enforcement action, or a commentary on how a specific AI tool handles user data, all demonstrate initiative and understanding in a way that a resume line cannot. You don't need to be an expert to write about something you're learning. Writing about it is usually how you learn. Not sure where to start?

A few concrete places worth trying:

- **Pitch The Privacy Advisor directly⁶.** IAPP accepts guest submissions from members and non-members alike, and getting published there carries real weight with people already in the field.
- **Law reviews and law journals** are more open to outside submissions than people expect, especially from students and early-career professionals looking to build a paper trail before their first privacy role.
- **Start a blog, even a small one.** It doesn't need traffic to matter. What matters is having a body of writing you can point to the next time someone asks what you actually know.
- **LinkedIn is the lowest-effort place to start.** A short post breaking down a new regulation or a recent enforcement action takes an afternoon, not a month, and it's often the very first thing a recruiter sees.

7.3 | Speak

Speaking at a small local event counts. It shows up on a resume, gives you something to talk about in interviews, and puts you in the room with people who might hire you later.

A few concrete places worth trying:

- **Local IAPP KnowledgeNet chapters.** Volunteer-led, in over 160 locations worldwide, and always looking for members to present a case study or walk through a recent regulatory update. Your local chapter is also free to join as an IAPP member.
- **IAPP conference calls for proposals.** Events like Privacy. Security. Risk. + AI Governance Global and the IAPP Summit open calls for speaking proposals to anyone, not just seasoned experts. Submitting is itself a credential, even if the talk doesn't get selected.
- **Internal company presentations.** Offer to walk your team through a new regulation or a recent enforcement action at a lunch-and-learn. It costs nothing to propose, and it's often the fastest way to be seen as "the privacy person" internally before you have the title.

7.4 | Network

Online communities are worth following too. Forums and groups across social media platforms are full of people asking these exact questions in real time, career changers, students, and professionals comparing notes on what actually worked for them. Reaching out directly to someone whose career path you admire, for a short informational call, also counts as networking and tends to be more useful than it sounds.

⁶International Association of Privacy Professionals. (2024). *Write for the IAPP*. IAPP. [Write for the IAPP](#)

A few concrete places to start:

- **IAPP Affinity Groups.** Independent, member-organized communities around shared interests or identities within privacy (cybersecurity crossover, legal specialists, and more). Anyone with a LinkedIn account can join; no IAPP membership is required.
- **Women in Security and Privacy (WISP).** A nonprofit network focused on mentoring, events, and career advancement for women in the field, open to join directly through their site.
- **LinkedIn, directly.** Comment thoughtfully on posts from people doing the work you want to do, or send a short, specific message asking for 15 minutes. Most privacy professionals remember what it was like to be the one asking.

7.5 | Take CLEs and Continuing Education

If you're coming from a legal background, look for continuing legal education credits focused on privacy or AI law. If you're from an accounting background, you might find continuing education classes focused on privacy audits. They're often low-cost or free through your professional association or employer, and they allow you to gain knowledge about the subject matter before committing to a wholesale career change.

A few concrete places to look:

- **Your state bar's CLE catalog.** Most state bars now list privacy and AI law as an approved CLE category, and many programs are free or low-cost for members.
- **IAPP training and web conferences.** Many of IAPP's own webinars and training sessions are pre-approved for CPE credit, so you can build privacy knowledge and satisfy your existing licensing requirements at the same time.
- **AICPA & CIMA CPE courses on SOC 2's privacy criteria.** If you're coming from accounting or audit, these courses walk through how privacy fits into the SOC 2 framework, a natural bridge if you're already familiar with audit work.

**Write****Speak****Network****Take CLEs/
Continuing
Education**

7.6 | Make It Count



LINKEDIN
Example
headline



BEFORE

“

IT Professional at
[Company]

”

“

Compliance Specialist

”



AFTER

“

IT Professional, CIPT |
Integrating Privacy Into
Systems by Design

”

“

Compliance Specialist,
CIPM | Building Effective
Privacy Programs From
Regulatory Requirements

”

- Add a “Licenses & Certifications” entry with the credential’s full name, for example “Certified Information Privacy Technologist (CIPT), IAPP.” This is what recruiter search filters actually match on.

Update your resume



RESUME
Example credential
or bullet



BEFORE

“

Certified Information
Privacy Manager (CIPM)

”



AFTER

“

CIPM, applied to build
[Company]’s first formal data
retention policy, reducing audit
findings by [X]

”

- Newly certified with no project to point to yet? That’s fine. Pair the certification with a concrete skill instead: “CIPM certified, with hands-on experience translating GDPR requirements into internal process documentation.”

What to say in an interview

Prepare one real example for each of these before you walk in:

- A time you had to explain a privacy or compliance requirement to someone outside your field.
- A time you had to make a judgment call without a perfect answer in the regulation.
- Why you chose this certification path over another. This is where your own story becomes your answer.

Your first 30 days as a certified professional

- Join your local privacy community. IAPP KnowledgeNet chapters exist in over 160 locations worldwide. They are free to attend and full of people hiring or being hired.
- Post about it once, genuinely. A short post about why you pursued the certification gets more attention than an announcement alone.
- Set a job alert using the certification's exact name, not just "privacy jobs." It's often the exact keyword recruiters filter by.
- Not job hunting yet? Tell your manager anyway. Certifications are one of the lowest-risk ways to open a conversation about a title change.

7.7 | Build Your People Skills

Every certification proves you know the material. What actually gets you hired, and promoted, is evidence that you can explain a dense requirement to someone who has never read it, and that people in other departments trust you enough to loop you in before they launch something, not after. Privacy work is inherently cross-functional, and none of that gets easier just because you passed an exam.

A few concrete ways to build it deliberately:

- **Practice translating jargon down.** Take one requirement you understand well and explain it to a friend outside the field in under two minutes, without using the word "compliance."
- **Volunteer for the meeting nobody wants.** Sitting in on a marketing campaign review or an engineering sprint planning session teaches you more about influence and timing than any course will, and it's usually an easy yes for whoever you ask to join.
- **Ask for feedback on how you communicate, not just what you know.** A mentor or manager who tells you an email came across as blocking rather than helping is handing you the exact skill employers are hiring for.

SECTION 8

Landing Your First (Or Next) Job in Privacy

Certifications and experience open doors for you, but they don't get you the job on their own. This section is about the practical mechanics: what employers are actually screening for, where the real opportunities are posted, what the current market looks like, and a few less obvious paths worth knowing about, like fellowships.

8.1 | What Do Employers Actually Want To See?

Hiring managers in privacy aren't looking for a perfect resume. They're looking for evidence that you can do three things: understand a requirement, translate it into action, and communicate it to people outside your field. Everything on your resume should point back to one of those three.

A few quick fixes that make a real difference:

- Lead with outcomes, not duties. "Managed vendor privacy reviews" says less than "Reviewed 40+ vendor contracts for GDPR compliance, flagging 12 for renegotiation."
- Name your certifications exactly, and early. If you're CIPP/US certified, that should appear near your name or job title, not buried in a skills list at the bottom.
- Translate your old job into privacy language. An employment attorney doesn't need a new resume; they need the same experience reframed. "Advised on employee data collection practices" is more relevant to a privacy recruiter than "handled employment litigation," even if both are true of the same job.
- Include one line about why. A short line about why you're moving into privacy, in a cover letter or LinkedIn summary, does more work than people expect. Hiring managers read a lot of resumes that could belong to anyone. A specific reason makes you memorable.

8.2 | Where Do I Find Jobs?

Start with [Privacy Bootcamp's job board](#), built specifically for privacy and AI governance roles, with current listings from companies like Figma, Postman, and Anduril, many of them noting which certification is preferred for the role.

Beyond that, a few resources worth checking regularly:

- IAPP's job board, one of the largest privacy-specific listings available, often includes roles not posted anywhere else.
- Company career pages directly, especially at large tech companies, banks, and healthcare organizations, which often have dedicated privacy or AI governance teams with steady hiring needs.
- KnowledgeNet chapter events, where roles are sometimes shared before they're posted publicly at all.

8.3 | Fellowships and Internships Worth Knowing About

Fellowships are one of the more overlooked ways into this field, especially for recent law graduates or people early in their careers.

A few of the most prestigious and well-known fellowships worth researching are:

- IAPP Westin Fellowship, a one-year, U.S.-based fellowship for research and scholarship in privacy, AI governance, and digital responsibility. It is open to applicants from any academic discipline.
- EPIC Law Fellowship, a one-year position at the Electronic Privacy Information Center in Washington, DC, working on legal research, litigation, and advocacy across areas like consumer privacy and surveillance oversight.
- Future of Privacy Forum Policy Fellowship, a one-year public interest fellowship for recent law graduates, focused on translating complex privacy and AI policy issues for a broad audience.
- CalPrivacy Honors Privacy Fellowship, a year-long placement in the Legal Division of the California Privacy Protection Agency (CPPA), open to 3L law students, LLM candidates, and recent graduates awaiting bar results. Fellows work directly on the agency's rulemaking process, gaining hands-on exposure to how a state privacy regulator actually operates.

These are not the only options. Several law firms and state attorney general offices run their own privacy or cybersecurity fellowship programs as well, and new ones open most years. For that reason, it's worth checking directly with organizations you're interested in, even if nothing is posted right now.

Internships are worth pursuing too, and unlike most fellowships, they don't require a law degree, which makes them one of the more accessible entry points into the field. Larger tech companies, banks, and healthcare organizations with dedicated privacy teams often bring on summer interns, sometimes through a formal, well-publicized program, and sometimes on a case-by-case basis if you simply reach out and ask. The work itself tends to be more substantive than the word "intern" suggests. Privacy interns are often pulled into real vendor reviews, data mapping exercises, or early-stage AI governance projects, not just administrative support, since privacy teams are usually small and genuinely need the extra hands.

If you're a student, your school's career office is usually the fastest route in, but it's also worth reaching out directly to a company's privacy or legal team on LinkedIn, even if no internship is formally posted. If you're changing careers, a short-term or part-time internship can also work as an entry point, even if it means stepping back in title or pay for a semester. What you're really trading for is the thing that's hardest to get otherwise: a real project, on a real team, that you can point to the next time you apply for a full-time role.

SECTION 9

There is No Single Path

By now, one thing should be clear: there is no single way to build a career in privacy. There is no one degree, no one certification, no one job title that defines what this profession looks like. That might feel unsettling if you're looking for a clear map. But it's also the reason this field has room for so many different kinds of people, and so much room to grow.

Take privacy law as one example. A law degree can take you toward private practice at a firm, advising clients on compliance and risk. It can take you in-house, working as counsel inside a single company, embedded in the products and decisions you're advising on. It can take you into academia, teaching and researching the next generation of privacy questions before the law has caught up to them. It can take you into government, shaping the regulations everyone else in the field eventually has to follow. Or it can take you into consulting, moving between organizations and industries instead of settling into one. Same degree, same starting certification, four or five entirely different careers.

The same is true across every path in this guide. Someone with a technical background might spend their career deep inside one company's engineering team, or move into consulting, building privacy programs for organizations that don't have the in-house expertise yet. Someone in program management might stay operational for their whole career, or use that foundation to move into AI governance as it continues to grow. There is no wrong direction here, only different ones.

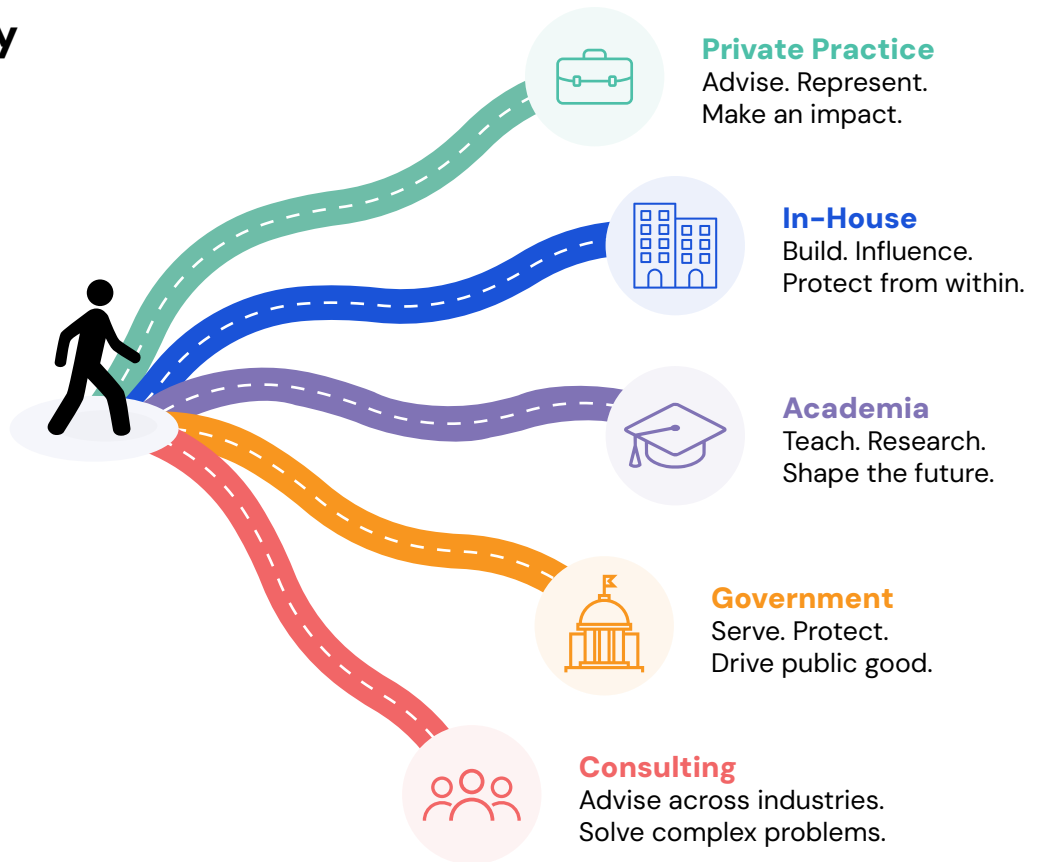
What makes this moment particularly interesting is that the field itself is still being defined, largely because of AI. That means the paths described in this guide are not fixed. New roles are being created faster than job descriptions can keep up with them, and the people shaping what those roles look like are, in many cases, the same people reading a guide like this one right now. If you're ambitious, that's not a downside. It's an opening. A field this young rewards people willing to build the role they want, instead of waiting for someone else to define it first.

Wherever you start, whichever path you choose, the goal isn't to find the one right way in. It's to find **your** way in.

One Path, Many Destinations.

Your privacy career can take many forms.

You are starting here. →



SECTION 10

Resources for Building a Career in Privacy and AI Governance

Ways to build experience and visibility

- Write for The Privacy Advisor — <https://iapp.org/news/write-for-us>
- IAPP KnowledgeNet Chapters — <https://iapp.org/connect/communities/chapters/>
- Speak at an IAPP Conference — <https://iapp.org/conference/speak-at-an-iapp-conference/>
- IAPP Affinity Groups — <https://iapp.org/connect/communities/affinity-groups/>
- Women in Security and Privacy (WISP) — <https://www.wisporg.com/>
- IAPP Continuing Privacy Education (CPE) — <https://iapp.org/certify/cpe/>
- AICPA & CIMA SOC 2 Privacy CPE Courses — <https://www.aicpa-cima.com/cpe-learning/publication/soc-2-reporting-on-an-examination-of-controls-at-a-service-organization-relevant-to-security-availability-processing-integrity-confidentiality-or-privacy>
- Privacy Bootcamp Article: “Privacy Law Certification: The PLS Designation” — <https://www.privacybootcamp.com/Resources/Article/Privacy-Certification-for-Lawyers-PLS-Designation>
- Privacy Bootcamp Quiz: “Which IAPP Certification Is Right for Me?” — <https://www.privacybootcamp.com/Resources/WhichIAPPCertForMe>

Formal education programs

- Carnegie Mellon — Master of Science in IT, Privacy Engineering (MSIT-PE) — <https://privacy.cs.cmu.edu/masters/index.html>
- Harvard Online — Data Privacy and Technology — <https://harvardonline.harvard.edu/course/data-privacy-technology>
- eCornell — Data Security and Privacy Policy Certificate — <https://ecornell.cornell.edu/certificates/financial-management/data-security-and-privacy-policy/>

Privacy and AI Governance Certifications

IAPP

- CIPP (Certified Information Privacy Professional) — <https://iapp.org/certify/cipp>
- CIPM (Certified Information Privacy Manager) — <https://iapp.org/certify/cipm>
- CIPT (Certified Information Privacy Technologist) — <https://iapp.org/certify/cipt>
- AIGP (Artificial Intelligence Governance Professional) — <https://iapp.org/certify/aigp>

ISACA

- CDPSE (Certified Data Privacy Solutions Engineer) — <https://www.isaca.org/credentialing/cdpse>
- CISA (Certified Information Systems Auditor) — <https://www.isaca.org/credentialing/cisa>
- CISM (Certified Information Security Manager) — <https://www.isaca.org/credentialing/cism>
- AAIA (Advanced in AI Audit) — <https://www.isaca.org/credentialing/aaia>

ISC2

- CISSP (Certified Information Systems Security Professional) — <https://www.isc2.org/certifications/cissp>
- CGRC (Certified in Governance, Risk and Compliance) — <https://www.isc2.org/certifications/cgrc>

PECB

- ISO/IEC 42001 Lead Implementer — <https://pecb.com/en/education-and-certification-for-individuals/iso-iec-42001>

Organizations worth following

- IAPP (formerly, the International Association of Privacy Professionals) — <https://iapp.org/>
- Future of Privacy Forum (FPF) — <https://fpf.org/>
- Electronic Privacy Information Center (EPIC) — <https://epic.org/>
- ISACA — <https://www.isaca.org/>
- ISC2 — <https://www.isc2.org/>

Job Boards and Job Search

- Privacy Bootcamp Job Board — <https://www.privacybootcamp.com/Resources/Jobs>
- IAPP Job Board — <https://jobs.iapp.org/>
- IAPP KnowledgeNet Events — <https://iapp.org/resources/topics/knowledgenet/>
- LinkedIn Jobs — <https://www.linkedin.com/jobs/>

Scholarships and professional development programs

- IAPP Westin Fellowship — <https://iapp.org/about/personnel/fellowships/>
- EPIC Law Fellowship — <https://epic.org/careers/>
- Future of Privacy Forum Fellowships — <https://fpf.org/about/career-opportunities/>
- CalPrivacy Honors Privacy Fellowship — https://cppa.ca.gov/about_us/jobs.html