IAPP Women Leading Privacy Web Conference

The Great Pivot: From Career Transition to Thriving as a Privacy Professional – An IAPP WLP FAQ for Women Transitioning into Privacy

Introduction

Breaking into or advancing in the privacy field requires a mix of regulatory knowledge, practical skills, and networking. During the IAPP Women Leading Privacy Web Conference, *"The Great Pivot: From Career Transition to Thriving as a Privacy Professional,"* industry experts answered pressing questions on how to navigate this evolving landscape. This FAQ compiles their actionable advice on overcoming entry barriers, gaining hands-on experience, and mastering non-legal and AI governance tracks.

Breaking into Privacy & Gaining Practical Experience

Q: As a career changer with a privacy bootcamp background and preparing for the CIPP/E, what are the best platforms to find entry-level remote jobs, and how can I gain hands-on operational experience in the meantime?

A: First, the CIPP/E is an excellent anchor; pair it with the CIPT (Certified Information Privacy Technologist) if you have a technical background, or CIPM if you lean operational. To look for experience and roles, job boards with strong privacy listings include the IAPP Career Central, LinkedIn, Indeed, Glassdoor, and Wellfound (AngelList). These are particularly good for start-up and scale-up privacy roles that welcome career changers.

For ways to build hands-on experience without a formal role, volunteer your privacy skills to a non-profit or community organisation, contribute to open-source privacy tools or documentation on GitHub, use free tiers of tools like OneTrust or Osano to practice building consent flows and data inventories, then document that as portfolio work.

Another thing to do is write case-study analyses of real GDPR or FTC enforcement decisions and publish them on LinkedIn or a personal blog. As a member, join the IAPP KnowledgeNet chapter in your region as many chapters host volunteer roles, mentorship pairing, and local employer connections.

Lead with your transferable skills such as risk, analysis and communication, and frame every project, no matter how small, as evidence of privacy practice.

Q: For someone coming from a regulatory and investigations background, what would you recommend as the fastest way to gain practical privacy experience without already being in a dedicated privacy role?

A: The regulatory and investigations background is one of the strongest adjacent skillsets for privacy, and the translation is more direct than most people realise. The fastest routes to practical experience is volunteering or consulting for small organizations (offer to draft their privacy notice, conduct a simple data audit, or help them respond to a subject access request), and document every engagement.

Within your current role, propose taking on privacy-adjacent responsibilities (data retention, record-keeping compliance, or managing freedom-of-information requests if your organisation handles them).

Prepare for and take the CIPP/E or CIPP/US certification examination. Your regulatory background means you will absorb the legal framework quickly, and the credential provides the privacy-specific signal employers need.

Look for roles with titles like "compliance analyst," "data governance analyst," or "privacy and risk analyst" that bridge your current background with the privacy field as these are often more accessible entry points than roles titled "privacy professional."

Navigating Career Transitions (From Specific Backgrounds)

Q: As someone coming from a quantitative health research and biostatistics background, what would you advise as the most effective step to transition into governance roles?

A: Your background is genuinely well-positioned for privacy and governance as health data is among the most heavily regulated categories of personal data globally, and quantitative skills are rare in most privacy teams.

Your immediate highest-value step is to obtain the CIPP/US or CIPP/E (depending on your target market) and pair it with knowledge of HIPAA (if U.S.-focused) or the EU's Article 9 special categories framework. These credentials, combined with a research background, make you a strong candidate for health privacy analyst and data governance roles.

Frame your existing skills explicitly and target roles to enter the field. These would include Health data governance analyst, research data steward, clinical data privacy analyst, or privacy and compliance analyst at a health system, payer, biotech company, or government health agency.

Consider also pursuing the AIGP (Artificial Intelligence Governance Professional) if health AI is an interest. That intersection (health data and AI governance) is a high-demand, undersupplied skillset in 2026 and beyond.

Q: What of non-legal positions and pathways within Privacy?

A: Privacy is far broader than its legal roots, and some of the most in-demand roles today are entirely non-legal. Here is a map of the major non-legal pathways:

- Privacy engineering & technology - Privacy engineers embed data protection into product development, data pipelines, and architecture. They work on privacy-by-design, data minimisation, anonymisation, and access controls. A software or data engineering background transitions well here. The CIPT certification is tailored to this path.
- Privacy operations & programme management - Privacy ops professionals run the day-to-day engine of a privacy programme: managing Records of Processing Activities (ROPAs), handling Data Subject Access Requests (DSARs), coordinating Data Protection Impact Assessments (DPIAs), and maintaining vendor risk registers. The CIPM is the certification of choice here.
- AI governance & ethics - Professionals who assess AI systems for fairness, transparency, and data risk. This intersects heavily with privacy and is one of the fastest-growing adjacent fields. The IAPP's AIGP certification was designed specifically for this role.
- Privacy analytics & data governance – Data professionals who manage data classification, retention, lineage, and quality in ways that support compliance. Often sits within data engineering or BI teams.
- Privacy consulting & advisory - Working for a consultancy to advise clients on building or improving their privacy programmes. This does not require a legal background; deep operational and programme experience is the primary qualification.
- Training & awareness – Designing and delivering privacy training for employees across an organisation. Often housed in HR, L&D, or the privacy team itself.

The common thread in all these paths is regulatory literacy (knowing what the rules require) combined with a domain-specific skill (engineering, analytics, project management, communication)

Early-Career Job Market Challenges & Strategy

Q: How can an early-career privacy professional overcome the 'overqualified but under-experienced' trap, where they have designed privacy frameworks but get rejected for entry-level roles due to a lack of hands-on, daily operational experience?

A: The "overqualified but under-experienced" gap is a very real frustration right now. Recruiters often screen for specific operational keywords rather than evaluating your structural depth.

Here is how to navigate and overcome this barrier:

- Make the implicit more explicit on your CV: Shift your wording from high-level to tactical. For example, if you designed a ROPA or DSAR workflow, explicitly detail the operational mechanics, data mapping, and decisions required to build it. Prove you understand the groundwork.
- Target the right organizations: Look for "Privacy Analyst" or "Privacy Operations" roles at mid-to-large companies. Alternatively, target consultancies and advisory firms; they heavily value candidates who know how to build programs from scratch for clients.
- Bypass the ATS via Networking: Automated keyword filters will continue to screen you out. Connect directly with hiring managers and privacy leaders through LinkedIn, IAPP KnowledgeNet, and local privacy communities as mentioned before. They understand the value of your background.
- Consider Short-Term Contracting: Taking a brief operational contract at a larger firm can quickly check the remaining "tactical experience" boxes on your resume, making your overall profile highly competitive.

Mid-to-Senior Career Advancement & Legal vs. Non-Legal Tracks

Q: If I already have several years of experience as a privacy professional and in AI governance, will I need a law degree to advance my career goals?

A: In most cases, no, but the answer depends on your long-term career goals. A law degree is not a prerequisite for advancing in privacy, including at senior and leadership levels. The field has matured significantly, and employers now recognise a wide range of expertise pathways as answered in a previous question.

What matters more than a JD at the senior level is a demonstrable combination of regulatory literacy, cross-functional leadership, and technical understanding. Your AI governance experience is particularly valuable right now, as organisations are actively searching for professionals who bridge privacy and AI risk, a skillset that remains scarce.

Where a law degree (or in-house legal counsel background) does help: roles explicitly titled "Privacy Counsel," "Associate General Counsel – Privacy," or DPO roles at large regulated organisations (financial services, healthcare), or working as a privacy attorney involved in litigation or civil matters that require legal sign-off authority. For these, a JD or a qualifying legal practitioner background is typically required. The process of earning a law degree or passing the bar can take considerable time, and starting earlier in your career may be advantageous. There are multiple routes and alternative ways to obtain a legal qualification later in your career too, and exploring them can help you choose the one that best aligns with your goals.

Alternatives that carry real weight at the senior level include IAPP's Fellow of Information Privacy (FIP) designation (a senior credential requiring demonstrated leadership and ongoing contribution to the field), a master's in privacy, data governance, cybersecurity law, or public policy (LLM in data protection is an option without a first law degree in some jurisdictions), and the AIGP (AI Governance Professional) certification from IAPP. If your goal is Chief Privacy Officer or VP-level at a technology company or consultancy, a law degree is rarely required. If it's General Counsel or privacy litigation, then yes, the path runs through law school.

Intersection of Privacy, AI Governance, and New Regulations

Q; To what extent are privacy professionals and legal counsels actively absorbing AI governance and new digital regulations (like the DSA/DMA) into their traditional remits, and what does that integration look like in practice?

A: Privacy teams have become the natural "first responders" for AI governance and new regulations (like the DSA/DMA) because they already own the organization's data compliance architecture.
In practice, this integration happens across three main areas:

- Upgrading Risk Assessments: Privacy counsels are expanding standard Data Protection Impact Assessments (DPIAs) to include algorithmic bias, model-training transparency, and data scraping risks.
- The DSA/DMA Overlap: Privacy pros are handling the cross-over rules. For example, auditing user interfaces for “Dark Patterns” (banned by the DSA) directly overlaps with managing cookie banners and consent under GDPR.
- The "DPO" Conflict of Interest: Under the GDPR, a Data Protection Officer must remain an independent auditor. If a DPO helps design an AI system, they create a conflict. To solve this, larger firms are creating a distinct “AI Governance Officer” role, while smaller firms rely on the privacy team to manage both by aligning tightly with engineering.

Ultimately, privacy is no longer just about protecting data; it has evolved into broader governance over how automated systems and algorithms use that data.

Privacy Tools & Technology

Q: What privacy tools are mostly applicable for use?

A: The privacy technology landscape has consolidated around a core set of platforms and tools. Here is a practical overview:

Privacy programme management platforms (most widely used in enterprise): These include OneTrust, TrustArc, Osano and Securiti.ai .
Data discovery & classification: BigID and Varonis (used for discovering where personal data lives across an organisation's systems and classifying it by sensitivity).
For learning and day-to-day reference, IAPP's Data Guidance covers 300+ jurisdictions, which is essential for tracking what laws apply where.

Post-Webinar Networking & Panelist Follow-up

Q: How can we connect with the panelists outside this webinar, and would you be open to connecting on LinkedIn and answering future questions?

A: The perspectives shared on the panel were incredibly valuable, and for anyone who would love to learn more about the panelists' work, or stay connected beyond this webinar, below are the networking details shared by the moderator and panelists:

- Antoinette Esslfie CIPP/US, CIPM, FIP (Moderator)
- Paulina Paczala AIGP, CIPP/US
- Prerna Bhushan
- Sofiya Brutsyak CIPP/E

Conclusion

The core takeaway from "The Great Pivot" is that modern privacy thrives on diverse, non-legal backgrounds. As data protection expands into AI governance, your unique transferable skills are highly valuable. By building a practical portfolio, mastering core tools, and staying active in communities like the IAPP, you can successfully launch and scale your career.