iapp

Salary and Jobs Report 2025–26

Privacy, AI Governance and Digital Responsibility

Contents

What's inside?

Key findings ..... *iii*

Executive summary ..... *iv*

Introduction ..... *vi*

I. The impactof digitalgovernance 1

II. Role-specific salary ranges 5

III. Total financialcompensationpackage 19

IV. Nonfinancialbenefits 24

V. Impact ofcertification 26

VI. Movers and shakers 28

VII. What's next? 31

Contacts 34

Key findings

$200,000	The global average total compensation reported across privacy, AI governance and cybersecurity roles
$280,000	The average base salary for CPOs
$190,000	The average base salary for AI governance legal and compliance professionals
$190,000	The average salary in the highest paying region is the U.S., paying 52% higher than Oceania and 69% higher than Europe
17%	The average bonus is 17% of base salary.
80%	Salary increases were secured by 80% over the past 12 months.
16%	Those that added additional digital governance responsibilities earned 16% more than those that hadn't added any digital governance responsibilities.

Executive summary

Transparency over pay continues to be vitally important

The financial wellbeing of employees is currently in flux. Global salaries and job security are directly impacted by interconnected political and economic factors.

The current geopolitical climate and evolving economic policies have been exerting significant influence on salary budgets and onward compensation available to employees. The era of post-COVID-19 pandemic salary growth may be slowing with labor costs now potentially inflated due to persistent inflationary pressures and a competitive talent market. Geoeconomic fragmentation and geopolitical tensions are likely to translate into business models transforming to account for trade restrictions, supply chain disruptions and broader policy uncertainty.

This highlights why now, more than ever, it is vital for professionals to make smart career choices. Salary and compensation are crucially important. However, talking about pay remains tricky. A variety of reasons persist – whether it's the social stigma around salary discussions, barriers to trustworthy dialogue, regulations preventing collusion, the desire for confidentiality over pay or strategic ambiguity by organizations to maintain competitiveness.

A survey conducted by recruitment website Glassdoor identified that 70% of surveyed employees across seven countries believe salary transparency is beneficial for employee satisfaction; on the other hand, only 36% identified that their organization internally discloses salaries. This despite 62% of employees willing to be transparent about salary information if they could do so anonymously.

This year's salary report presents data for those working on privacy only, artificial intelligence governance only, both privacy and AI governance and those with additional digital governance responsibilities. This data offers the opportunity to hold informed and transparent discussions over pay through using the data in this report to benchmark individual pay and and organizational pay structures.

Reading the report

1 The impact of digital governance

To what extent have salaries kept pace with the increasingly complex risk environment and digital governance required to address this?

2 Role-specific salary ranges

How do salaries vary by an individual's role?

3 Total financial compensation package

What does the average compensation package look like?

4 Nonfinancial benefits

What additional benefits are offered to employees?

5 Impact of certification

To what extent does additional certification impact salaries?

6 Movers and shakers

How does job satisfaction vary amongst respondents? What would cause them to move roles?

7 What's next?

What are some potential next steps you could take after reading the report?



Introduction

Benchmarking the evolving profession

Since 2003, the IAPP has conducted a salary survey to help privacy professionals benchmark their salaries. This year's report continues the tradition of providing insights that help professionals and organizations benchmark salaries and total compensation, recognize the value of certifications, obtain a temperature check in the form of job satisfaction and likelihood of finding another job, and more.

We asked our global community to complete a 27-question salary survey. Over the course of six weeks from March to April 2025, more than 1,600 people from over 60 countries responded. This is the largest and most globally diverse response yet.

New to this year's report is the inclusion of AI governance professional salaries as well as insights and analysis on the impact to salary of working on other digital governance domains, such as cybersecurity law. The expanded scope of the report, consistent with the IAPP's mission, now serves a broader array of professions, all of which are critical to the governance of digital technology.

In this report, base salary refers to regular salary or wages, not including bonuses or other types of additional compensation. Total financial compensation refers to the base salary plus bonuses and other types of extra compensation. Neither base salary nor total compensation include the value of other employee benefits, such as health insurance policies.

Reading the data

This year's report provides data in a ranged format for ease of comparison. The type of data included in the report and how it was obtained is described below.

→ Quartile 1: Also known as the lower quartile (Q1), it represents the salary level below which 25% of the reported salaries for a specific job role fall. It defines the upper limit of the lowest quarter of the salary distribution.

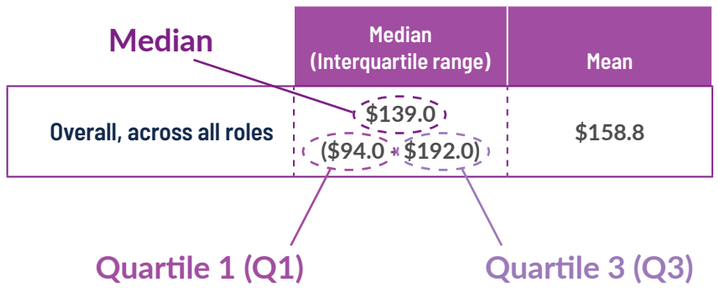
→ Median: The median salary is the midpoint of the salary distribution for a particular job role. When all reported salaries are arranged in ascending order, 50% of salaries are below the median and 50% are above. It serves as a robust measure of central tendency and is less sensitive to extreme salary values.

→ Quartile 3: Also known as the upper quartile (Q3), it represents the salary threshold below which 75% of reported salaries for a given job role fall. It defines the starting point of the highest quarter of the salary distribution.

→ Interquartile range: The difference (Q3-Q1) between the third quartile and the first quartile to quantify the spread of the middle 50% of salaries for a given job role. This provides a measure of the variability of typical salaries that is resistant to the influence of outliers.

→ Mean: The mean salary is the arithmetic average of all reported salaries for a specific job role. In this report, it is calculated as an adjusted mean by summing all individual salaries, excluding extreme outliers and dividing by the total number of remaining responses. The mean is a common measure of central tendency, though it can be affected by the highest and lowest salary values at the extremes.

The reporting on this data is as granular as possible while balancing issues around reidentification and small sample bias. Data from small samples is excluded to reduce the risk of identification and appears as grey in the tables.



New to this year's report is the inclusion of AI governance professional salaries as well as insights and analysis on the impact to salary of working on other digital governance domains, such as cybersecurity law. The expanded scope of the report, consistent with the IAPP's mission, now serves a broader array of professions, all of which are critical to the governance of digital technology.



Privacy &

The privacy profession is undergoing significant transformation; its already complex nature has been deeply impacted by the influence of artificial intelligence and the pressing need for strong AI governance. The IAPP Privacy Governance Report 2024 identified how privacy professionals are increasingly being tasked with tackling AI governance.

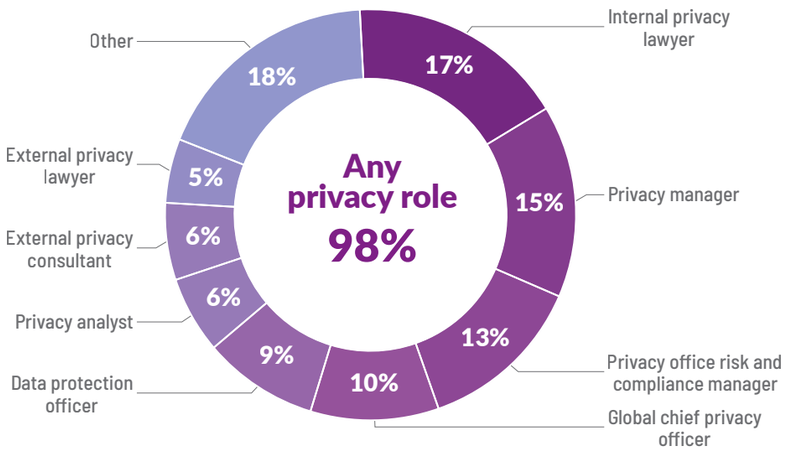
The 2024 report identified that approximately 68% of respondents said they had acquired additional responsibility for AI governance, 60% reported further responsibilities for data governance, 40% for cybersecurity and 37% for data ethics. Privacy professionals continue to deal with a surge in privacy regulations, evolving case law, increasing complexities of international data transfers in the global data economy and a steady stream of complex and sometimes conflicting regulatory guidance.

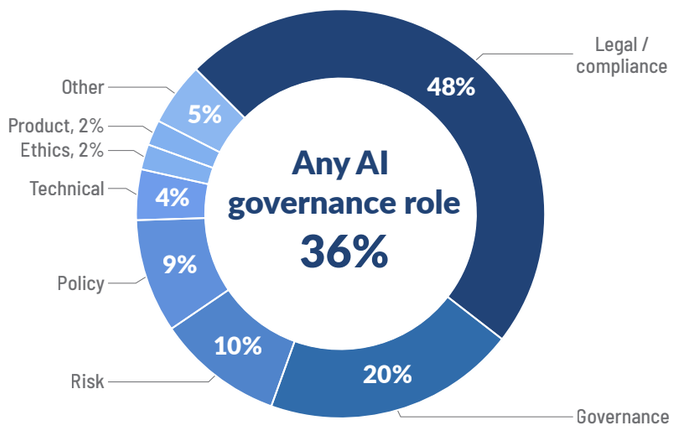
Layered on top of this is the need to understand and address the unique challenges presented by AI technologies. The complexity of this field requires its own specialisms and specialists that can navigate the ethical implications of AI, ensure responsible use of data within AI systems and understand the impact of AI on individual rights.

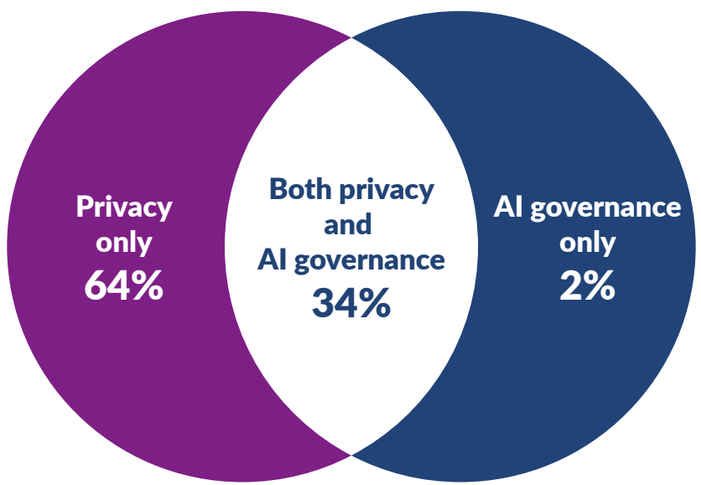
This year's salary report focuses on those working on privacy only, on AI governance only, working on both and those with additional digital governance responsibilities. Approximately 36% of this year's respondents had defined responsibilities for AI governance, while 98% of respondents had a formal privacy role. Of those respondents with AI governance roles, almost 1 in 2 worked in the legal/compliance domains, 1 in 5 in governance-focused roles and 10% on risk within AI governance.

The varied role continues when considering broader digital governance. More than half of all respondents had some responsibility for AI governance, 51% had responsibility for data governance and almost 1 in 3 were responsible for data ethics or cybersecurity as a regulatory compliance matter.

Breakdown of core responsibilities of respondents







Approximately 36% of this year's respondents had defined responsibilities for AI governance, while 98% of respondents had a formal privacy role. Of those respondents with AI governance roles, almost 1 in 2 worked in the legal/compliance domains, 1 in 5 in governance focused roles and 10% on risk within AI governance.

I. The impact of digital governance

Are evolving roles with increasingly diverse responsibilities paid more?

To what extent have salaries kept pace with the increasing complexity and expectations placed upon professionals? Long gone are the days when professionals working in this field could focus solely on a single regulation, only poring over the articles of the EU General Data Protection Regulation and accompanying regulatory guidance.

In 2025, professionals must contend with privacy, cybersecurity, AI governance, content moderation, product liability, intellectual property, accessibility, competition and online safety. Digital governance encompasses any combination of these domains and has increased in prominence. The need for coordination among these topics is clear, especially in an environment where there is greater geopolitical flux, increased pressure to tighten budgets and rapid developments in internal and external environments.

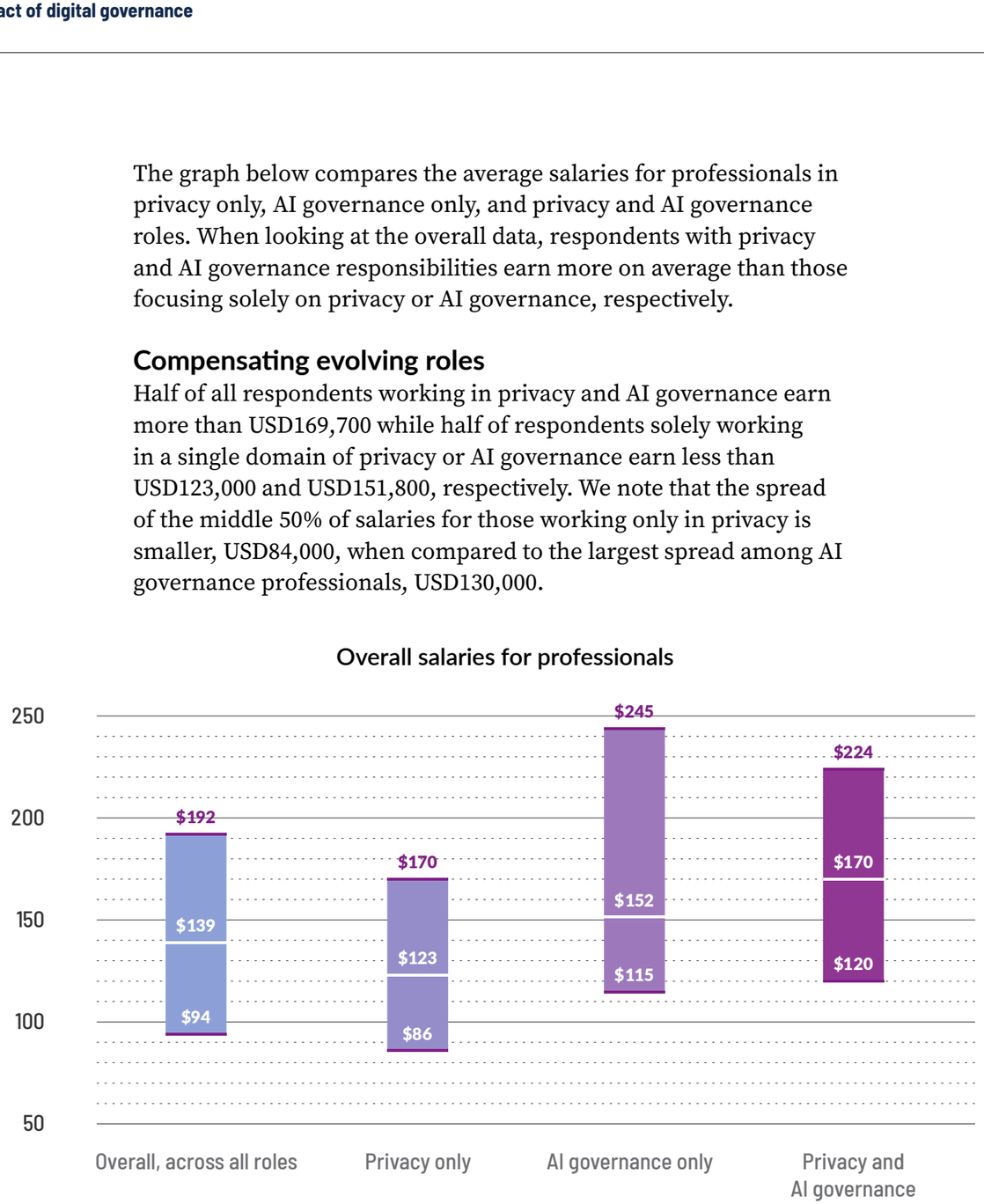
The first comparison we can make is comparing like-for-like data from previous salary surveys with this year's data. In 2025, the average adjusted base salary for a privacy pro in an internal role has seen a 1% increase from 2023 and an 8% increase from 2021. However, greater increases can be seen for roles with privacy and AI governance responsibilities.

The graph below compares the average salaries for professionals in privacy only, AI governance only, and privacy and AI governance roles. When looking at the overall data, respondents with privacy and AI governance responsibilities earn more on average than those focusing solely on privacy or AI governance, respectively.

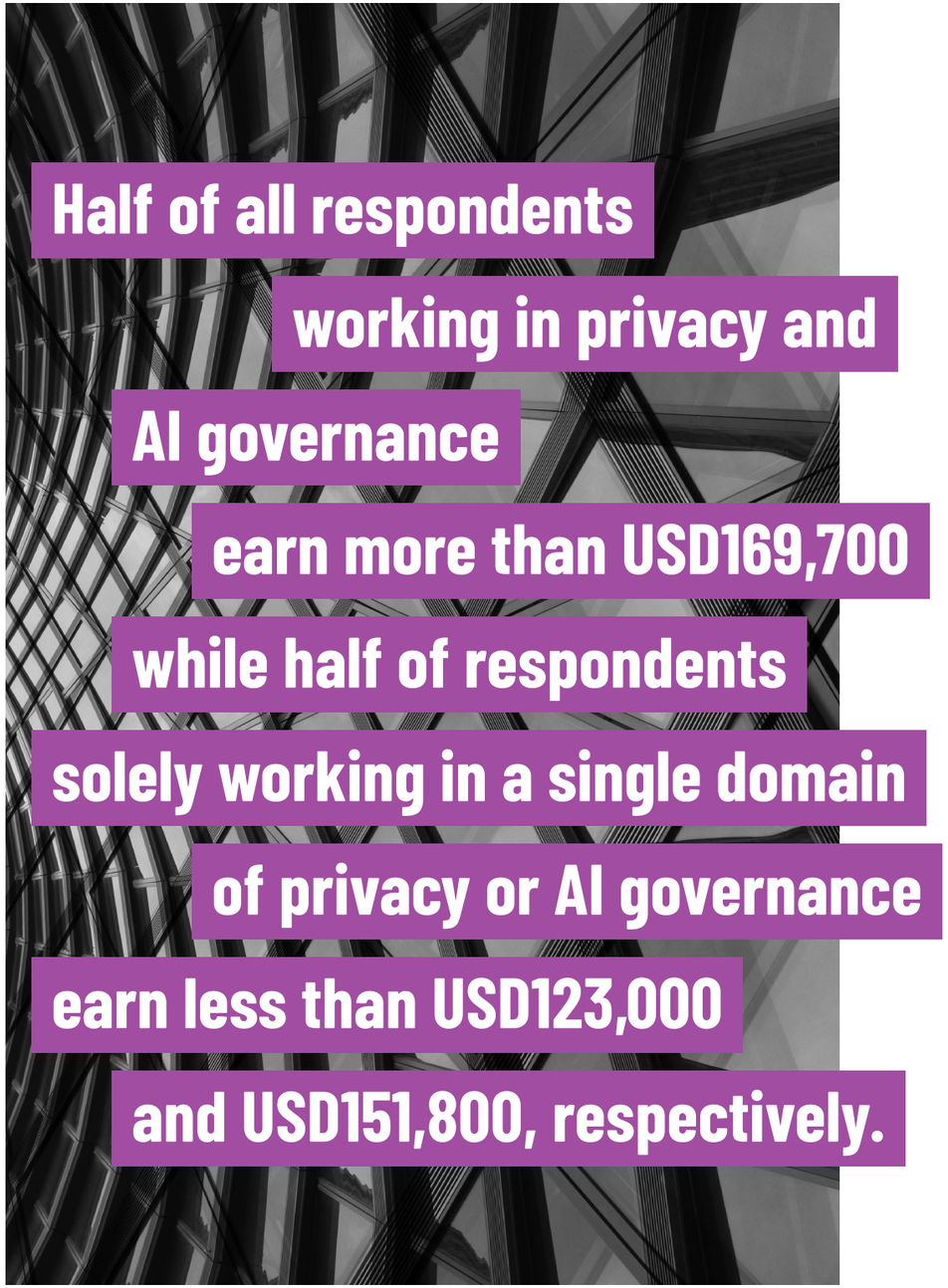
Compensating evolving roles

Half of all respondents working in privacy and AI governance earn more than USD169,700 while half of respondents solely working in a single domain of privacy or AI governance earn less than USD123,000 and USD151,800, respectively. We note that the spread of the middle 50% of salaries for those working only in privacy is smaller, USD84,000, when compared to the largest spread among AI governance professionals, USD130,000.

Overall salaries for professionals



The figures in these tables are base salary, with total compensation included on page 20. All figures are in thousands of U.S. dollars.



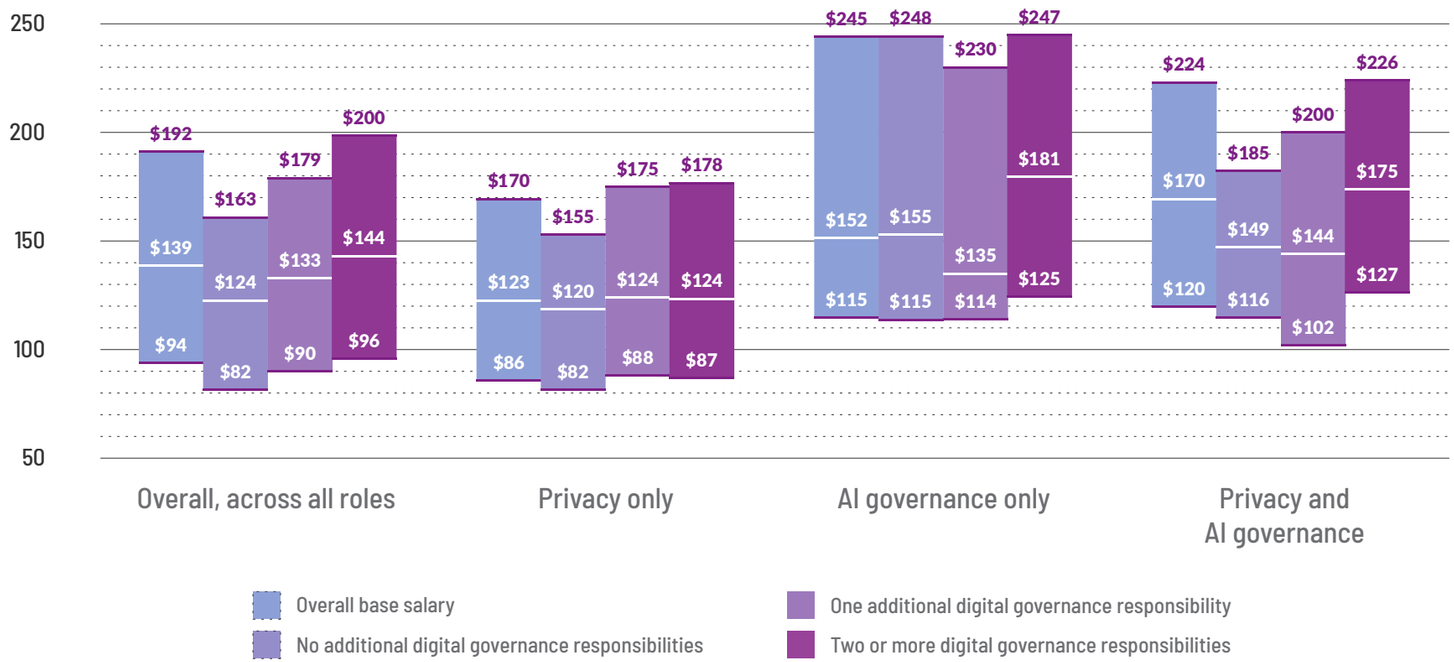
The chart below identifies how respondents have added additional responsibilities to their role. Of those respondents with AI governance responsibilities, a significant number (96%) also have privacy responsibilities with 63% having data governance and 45% having cybersecurity as a regulatory compliance matter as additional responsibilities. Multiskilled employees with expertise and ability to perform across multiple domains are becoming the norm rather than the exception.

To what extent are employers compensating employees for taking on additional responsibilities? The graph below identifies the reported salaries of those who have added other digital governance domains to their portfolio, such as data ethics, data governance and intellectual property.

Proportion of respondents that have responsibilities for additional domains

DOMAIN OF RESPONSIBILITY	Percentage of respondents
Privacy	96%
AI governance	54%
Data governance/data use/data as an asset	51%
Cybersecurity as a regulatory compliance matter	34%
Data ethics	27%
Consumer protection	17%
Platform liability	13%
Intellectual property	9%
Digital architecture and infrastructure	8%
Content moderation and online safety	6%
Human rights	6%
Product liability	5%
Competition/antitrust	3%

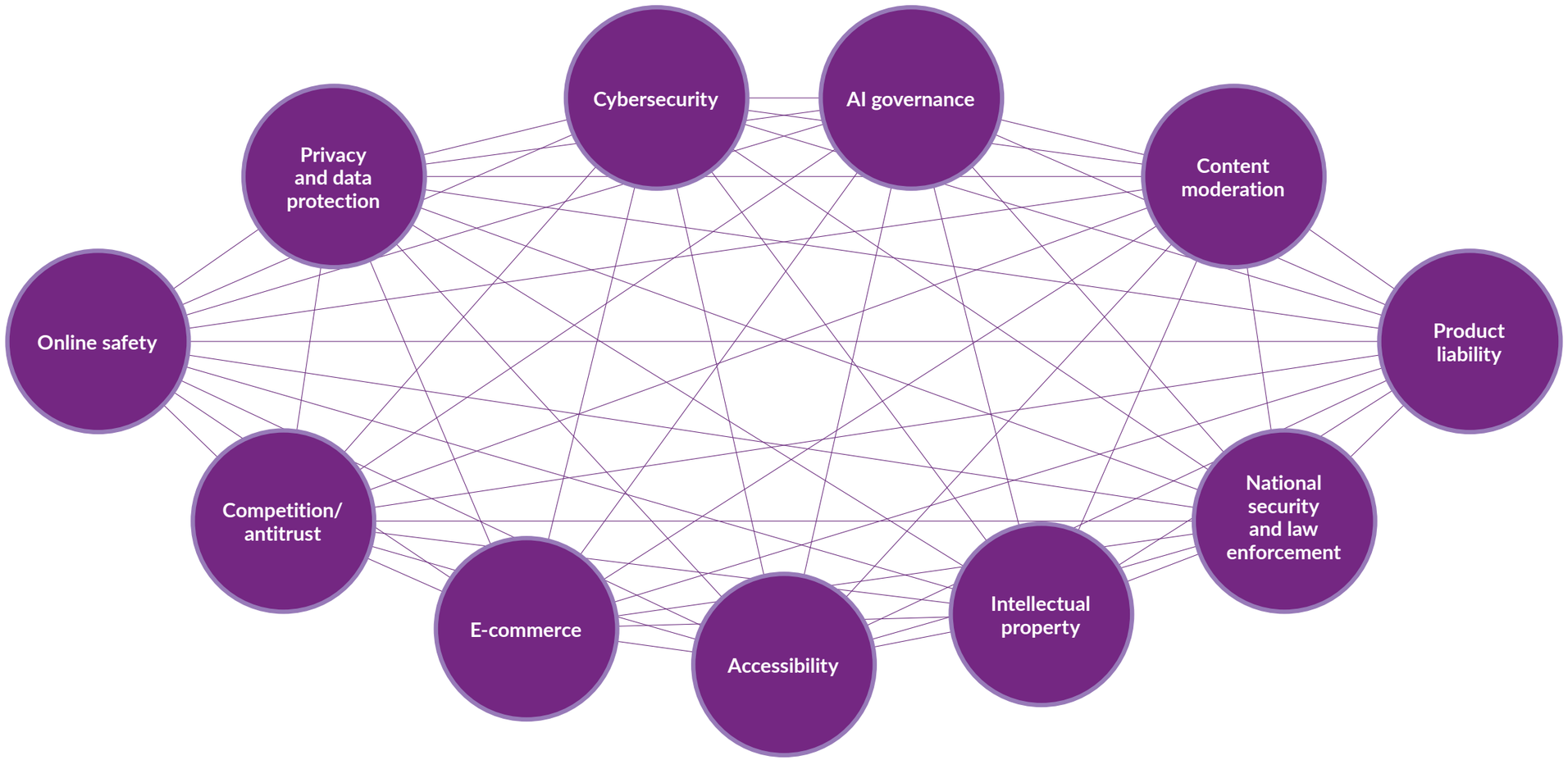
The impact of digital governance responsibilities on salary



As identified in the 2024 Organizational Digital Governance report, digital governance domains include a number of interrelated topics.

The data identifies that respondents with at least two additional digital governance responsibilities can expect to earn more than those with one additional responsibility. On average, salaries were USD30,000 higher for those with two or more digital governance responsibilities, while 25% of respondents with two or more digital governance responsibilities earned over USD200,000.

The matrix of digital governance domains



II. Role-specific salary ranges

Defining the roles that deliver

In order to capture AI governance as well as broader digital governance responsibilities, this year's survey sought to expand the scope beyond focusing solely on privacy roles. The definitions of the roles included in this year's survey are outlined on the next page.

PRIVACY

INTERNAL ROLES

- **Global chief privacy officer:** CPO for a global or multinational organization and may carry ultimate organizational responsibly for privacy
- **Chief privacy officer, country:** CPO for an organization with operations in one country
- **Regional privacy officer:** Supports the CPO delivering privacy across a region/geographic area, such as Europe, the Middle East and Africa
- **Data protection officer:** DPO for an organization
- **Privacy office risk and compliance manager:** Works on the privacy team delivering day-to-day privacy risk, operations and compliance activities
- **Privacy manager:** Works in the privacy team to deliver and/or manage delivery of day-to-day privacy activities
- **Privacy analyst:** Works in the privacy team to deliver day-to-day privacy activities
- **Internal privacy lawyer:** Provides internal support to organizations on the technical legal aspect of privacy regulations
- **Privacy champion or guru:** Individual assigned a percentage of their time — less than 25% to support an aspect of privacy, such as compliance officer in a market who is given some privacy responsibilities
- **Privacy engineer:** Covers engineers with responsibilities for areas such as privacy enablement, product ownership/design, coding and/or analytics
- **Cybersecurity professional:** Designs, develops and delivers on security for privacy

EXTERNAL ROLES

- **External privacy consultant:** Supports clients, design, develop, implement and outsourcing of operational privacy activities
- **External privacy lawyer:** Provides external support to organizations on the technical legal aspect of privacy regulations, such as breach, transfers or contracts

AI GOVERNANCE

For the purposes of this survey, AI roles were identified by theme rather than focusing on specific job titles. As job title nomenclature is still in early stages, it may be more helpful for organizations and individuals to compare to AI governance role categories rather than specific titles. The following domains were included:

- **Legal/compliance:** Supports compliance within the organization and ensures reporting requirements are fulfilled
- **Policy:** Designs policy changes and works to integrate regulatory requirements into internal policy and governance guidelines
- **Governance:** Operates AI governance framework within the organization
- **Ethics:** Conducts internal ethics assessments and ensures AI use complies with internal ethics codes
- **Risk:** Identifies and manages risks associated with AI systems
- **Technical:** Supports compliance with AI policy and governance requirements within data, model and IT infrastructure
- **Product:** Integrates AI governance and policy requirements into products offered by the organization



Base salary for privacy professionals by role

ROLE	Median (Q3 - Q1)
Global chief privacy officer	$215.0 ($156.0 - $291.0)
Chief privacy officer (country)	$149.0 ($109.0 - $196.0)
Regional privacy officer	$142.0 ($91.0 - $193.0)
Privacy office risk and compliance manager	$120.0 ($87.0 - $170.0)
Internal privacy lawyer	$176.0 ($135.0 - $225.0)
Privacy champion/guru	$137.0 ($105.0 - $163.0)
Privacy engineer	$145.0 ($110.0 - $200.0)
Data protection officer	$108.0 ($81.0 - $152.0)
Privacy manager	$105.0 ($78.0 - $145.0)
Privacy analyst	$92.0 ($63.0 - $107.0)
External privacy consultant	$121.0 ($79.0 - $174.0)
External privacy lawyer	$183.0 ($127.0 - $250.0)

The figures in these tables are base salary, with total compensation included on page 20. All figures are in thousands of U.S. dollars.

Base salary for cybersecurity professionals

	Overall
Cybersecurity professional	$152.0 ($127.0 - $190.0)

All figures are in thousands of U.S. dollars.

Privacy

The table to the left outlines the median salary and interquartile ranges of salary for surveyed roles.

The following highlights were identified:

Global CPOs, followed by internal privacy lawyers, are the highest paid roles. The median salary for both roles is higher than any other role. Over three quarters of global CPO respondents earned above USD156,000 while 75% of internal privacy lawyers earned above USD135,000.

CPOs with a global role earn more than those with a more country specific role. The median salary of a global CPO is USD66,000 higher than a country specific CPO and at least 50% of country specific CPOs earn less than 75% of global CPOs.

An external privacy lawyer's median salary continues to be higher than an internal privacy lawyer by approximately USD7,000. The spread of salaries for external privacy lawyers is USD123,000, USD33,000 higher than the spread for internal privacy lawyers at USD90,000.

Cybersecurity professionals earned a median salary of USD152,000, with a USD63,000 range for the middle 50% of respondents.

The median salary of a global CPO is USD66,000 higher than a country specific CPO and at least 50% of country specific CPOs earn less than 75% of global CPOs.

Industry differences in base salary

The following aggregated view groups industries to show a median salary, interquartile range and average salary by industry.

The defense, energy, manufacturing and logistics sectors, made up of aerospace and defense, agriculture and natural resources, chemicals, mining and materials, construction and engineering, manufacturing, oil and gas and transportation and logistics, had the highest average salary at USD203,000. The health care sector followed with an average salary of USD164,000. The government and education sector had the lowest average salary at USD120,000 and the lowest median salary at USD102,000.

The sector with the greatest spread in salaries were health care at USD120,000, technology at USD108,000 and finance at USD97,000, which suggests greater variability in the salaries of respondents working in these industries. Government and education had the narrowest spread in data with the middle 50% of salaries falling within a USD64,000 spread.

This can be broken down further by roles within each industry where possible. Data is excluded in small samples to reduce risk of identification.

Average salary by industry

	Overall	Technology	Finance	Health care	Retail, media and leisure	Defense, energy, manufacturing and logistics	Government and education	Business services, consulting and legal	Other
Median (interquartile range)	$139.0 ($95.0 - $190.0)	$150.0 ($101.0 - $209.0	$131.0 ($90.0 - $187.0)	$149.0 ($102.0 - $222.0)	$146.0 ($106.0 - $200.0)	$145.0 ($95.0 - $185.0)	$102.0 ($81.0 - $145.0)	$136.0 ($100.0 - $183.0)	$127.0 ($85.0 - $164.0)
Mean	$156.0	$159.0	$142.0	$164.0	$163.0	$203.0	$120.0	$148.0	$128.0

All figures are in thousands of U.S. dollars.

Base salary for privacy professionals by industry

	Overall	Technology	Finance	Health care	Retail, media and leisure	Defense, energy, manufacturing and logistics	Government and education	Business services, consulting and legal	Other
Global chief privacy officer	$215.0 ($156.0 - $291.0)	$202.0 ($150.0 - $283.0)	$220.0 ($169.0 - $300.0)	$268.0 ($230.0 - $355.0)	$245.0 ($133.0 - $300.0)	$183.0.0 ($140.0.0- $262.0)	$220.0 ($155.0 - $256.0)	$198.0 ($139.0 - $330.0)	
Chief privacy officer (country)	$149.0 ($109.0 - $196.0)	$121.0 ($90.0 - $275.0)	$155.0 ($114.0 - $217.0)	$150.0 ($102.0 - $206.0)	$179.0 ($134.0 - $238.0)	$160.0 ($89.0 - $217.0)	$122.0 ($106.0 - $164.0)		
Regional privacy officer	$142.0 ($91.0 - $193.0)	$100.0 ($72.0 - $164.0)	$147.0 ($98.0 - $184.0)	$151.0 ($120.0 - $247.0)	$139.0 ($103.0 - $144.0)	$150.0 ($106.0 - $194.0)		$164.0 ($79.0 - $221.0)	
Privacy office risk and compliance manager	$120.0 ($87.0 - $170.0)	$128.0 ($86.0 - $178.0)	$114.0 ($84.0 - $160.0)	$154.0 ($106.0 - $222.0)	$120.0 ($89.0 - $179.0)	$128.0 ($79.0 - $170.0)	$92.0 ($70.0 - $139.0)	$105.0 ($82.0 - $132.0)	$147.0 ($100.0 - $164.0)
Internal privacy lawyer	$176.0 ($135.0 - $225.0)	$180.0 ($139.0 - $235.0)	$183.0 ($127.0 - $217.0)	$160.0 ($140.0 - $227.0)	$190.0 ($148.0 - $223.0)	$170.0 ($91.0 - $220.0)	$140.0 ($100.0 - $208.0)	$170.0 ($102.0 - $205.0)	$174.0 ($146.0 - $190.0)
Privacy champion/guru	$137.0 ($105.0 - $163.0)	$141.0 ($106.0 - $181.0)							
Privacy engineer	$145.0 ($110.0 - $200.0)	$170.0 ($69.0 - $194.0)			$154.0 ($111.0 - $273.0)	$145.0 ($120.0 - $216.0)			
Data protection officer	$108.0 ($81.0 - $152.0)	$125.0 ($102.0 - $159.0)	$106.0 ($85.0 - $158.0)	$107.0 ($78.0 - $116.0)	$127.0 ($100.0 - $170.0)	$88.0 ($85.0 - $113.0)	$81.0 ($62.0 - $90.0)	$132.0 ($90.0 - $152.0)	$82.0 ($63.0 - $86.0)
Privacy manager	$105.0 ($78.0 - $145.0)	$106.0 ($67.0 - $154.0)	$101.0 ($59.0 - $136.0)	$110.0 ($92.0 - $145.0)	$111.0 ($84.0 - $145.0)	$137.0 ($100.0 - $162.0)	$84.0 ($71.0 - $100.0)	$142.0 ($103.0 - $151.0)	$102.0 ($85.0 - $111.0)
Privacy analyst	$92.0 ($63.0 - $107.0)	$78.0 ($51.0 - $111.0)	$93.0 ($68.0 - $106.0)	$88.0 ($57.0 - $93.0)	$103.0 ($66.0 - $121.0)	$95.0 ($71.0 - $105.0)	$93.0 ($76.0 - $113.0)	$103.0 ($77.0 - $128.0)	
External privacy lawyer	$183.0 ($127.0 - $250.0)							$161.0 ($82.0 - $234.0)	

All figures are in thousands of U.S. dollars.

A number of trends can be highlighted from these results. Global CPOs working in the health care, finance and retail industries were among the most well-paid professionals with higher median salaries — 25% of respondents in each of these industries reported earning more than USD300,000. One industry grouping did not tend to rank highest for median pay across all roles. Across most industries, with government and education being the exception, privacy analysts could expect to get a healthy bump in salary on promotion to privacy manager. For instance, median salaries of those analysts working in the technology industry jumped from USD78,000 to USD106,000.

For cybersecurity professionals, the technology sector was the most lucrative. Half of respondents working in the technology sector earned more than 75% of those working in the government and education sectors.

Base salary for cybersecurity professionals by industry

	Overall	Technology	Finance	Health care	Retail, media and leisure	Defense, energy, manufacturing and logistics	Government and education	Business services, consulting and legal	Other
Cybersecurity professional	$152.0 ($127.0 - $190.0)	$184.0 ($145.0 - $205.0)	$149.0 ($140.0 - $200.0)			$127.0 ($96.0 - $182.0)	$110.0 ($100.0 - $162.0)		

All figures are in thousands of U.S. dollars.

For cybersecurity professionals, the technology sector was the most lucrative. Half of respondents working in the technology sector earned more than 75% of those working in the government and education sectors.

Operational demographics

The following aggregated revenue view groups responses into small, (those working in organizations with less than USD100 million in revenue), medium organizations (USD101 to 999 million), and large (greater than USD1 billion in annual revenue)

The trend identified in previous salary surveys persists: respondents working in larger organizations tend to have higher salaries. More than 50% of respondents working in organizations with greater than USD1 billion in annual revenue earned more than USD150,000 while only 25% of those working in organizations with less than USD100 million in annual revenue earned more than USD155,000.

The trend also holds true that larger organizations pay more across almost every role. Privacy analysts working in large organizations earn USD3,000 more at the median salary than those working in small organizations. The salary spread of the middle 50% is much broader at larger organization; there is a USD34,000 spread for privacy analysts in small organizations and a USD40,000 spread for privacy analysts in large organizations. At the global CPO level, 50% of respondents working in large organizations earned more than USD238,000, while only 25% of those working in small organizations earned more than USD196,000.

Base salary by organization size (annual revenue)

	Small — less than $100 M	Medium — $101 M to $999 M	Large — greater than $1 B
Median (interquartile range)	$105.0 ($79.0 - $155.0)	$129.0 ($89.0 - $185.0)	$150.0 ($106.0 - $205.0)
Mean	$128.0	$142.0	$174.0

All figures are in thousands of U.S. dollars.

Base salary across cybersecurity roles by organization size (annual revenue)

	Small — less than $100 M	Medium — $101 M to $999 M	Large — greater than $1 B
Overall	$105.0 ($79.0 - $155.0)	$129.0 ($89.0 - $185.0)	$150.0 ($106.0 - $205.0)
Global chief privacy officer	$186.0 ($96.0 - $196.0)	$208.0 ($139.0 - $255.0)	$238.0 ($159.0 - $300.0)
Chief privacy officer (country)	$110.0 ($88.0 - $153.0)	$140.0 ($96.0 - $214.0)	$161.0 ($131.0 - $198.0)
Regional privacy officer		$96.0 ($72.0 - $150.0)	$149.0 ($101.0 - $209.0)
Privacy office risk and compliance manager	$88.0 ($69.0 - $128.0)	$106.0 ($87.0 - $154.0)	$132.0 ($94.0 - $178.0)
Internal privacy lawyer	$138.0 ($102.0 - $180.0)	$176.0 ($130.0 - $226.0)	$183.0 ($144.0 - $230.0)
Privacy champion/guru	$106.0 ($50.0 - $115.0)	$136.0 ($120.0 - $139.0)	$158.0 ($137.0 - $181.0)
Privacy engineer			$162.0 ($120.0 - $216.0)
Data protection officer	$75.0 ($59.0 - $99.0)	$99.0 ($82.0 - $143.0)	$134.0 ($106.0 - $164.0)
Privacy manager	$90.0 ($78.0 - $105.0)	$100.0 ($65.0 - $135.0)	$115.0 ($81.0 - $149.0)
Privacy analyst	$90.0 ($60.0 - $94.0)	$91.0 ($55.0 - $110.0)	$93.0 ($71.0 - $111.0)
External privacy consultant	$111.0 ($73.0 - $170.0)	$106.0 ($80.0 - $159.0)	$126.0 ($103.0 - $200.0)
External privacy lawyer	$140.0 ($82.0 - $210.0)	$190.0 ($138.0 - $250.0)	$275.0 ($186.0 - $420.0)

All figures are in thousands of U.S. dollars.

Base salary across cybersecurity roles by organization size (annual revenue)

	Small — less than $100 M	Medium — $101 M to $999 M	Large — greater than $1 B
Overall	$105.0 ($79.0 - $155.0)	$129.0 ($89.0 - $185.0)	$150.0 ($106.0 - $205.0)
Cybersecurity professional	$160.0 ($135.0 - $175.0)	$152.0 ($96.0 - $190.0)	$149.0 ($128.0 - $198.0)

All figures are in thousands of U.S. dollars.

Base salary for privacy professionals by continent

	North America	Europe	Asia and Oceania
Global chief privacy officer	$256.0 ($192.0 - $300.0)	$158.0 ($121.0 - $202.0)	$189.0 ($130.0 - $283.0)
Chief privacy officer (country)	$161.0 ($127.0 - $206.0)	$85.0 ($66.0 - $109.0)	
Regional privacy officer	$156.0 ($124.0 - $200.0)	$103.0 ($79.0 - $164.0)	
Privacy office risk and compliance manager	$141.0 ($102.0 - $178.0)	$79.0 ($59.0 - $117.0)	$100.0 ($58.0 - $119.0)
Internal privacy lawyer	$190.0 ($145.0 - $229.0)	$127.0 ($87.0 - $175.0)	$155.0 ($123.0 - $271.0)
Privacy champion/guru	$138.0 ($110.0 - $165.0)		
Privacy engineer	$155.0 ($112.0 - $212.0)		
Data protection officer	$149.0 ($114.0 - $170.0)	$96.0 ($79.0 - $122.0)	$164.0 ($110.0 - $184.0)
Privacy manager	$124.0 ($99.0 - $151.0)	$74.0 ($58.0 - $95.0)	$89.0 ($69.0 - $144.0)
Privacy analyst	$95.0 ($76.0 - $113.0)	$52.0 ($48.0 - $67.0)	$63.0 ($50.0 - $77.0)
External privacy consultant	$140.0 ($110.0 - $186.0)	$91.0 ($67.0 - $136.0)	$110.0 ($91.0 - $197.0)
External privacy lawyer	$227.0 ($180.0 - $300.0)	$119.0 ($84.0 - $170.0)	

All figures are in thousands of U.S. dollars.

Base salary for cybersecurity professionals by continent

	North America	Europe	Asia and Oceania
Overall	$165.0 ($123.0 - $221.0)	$101.0 ($74.0 - $138.0)	$118.0 ($62.0 - $174.0)
Cybersecurity professional	$175.0 ($145.0 - $196.0)	$128.0 ($100.0 - $149.0)	

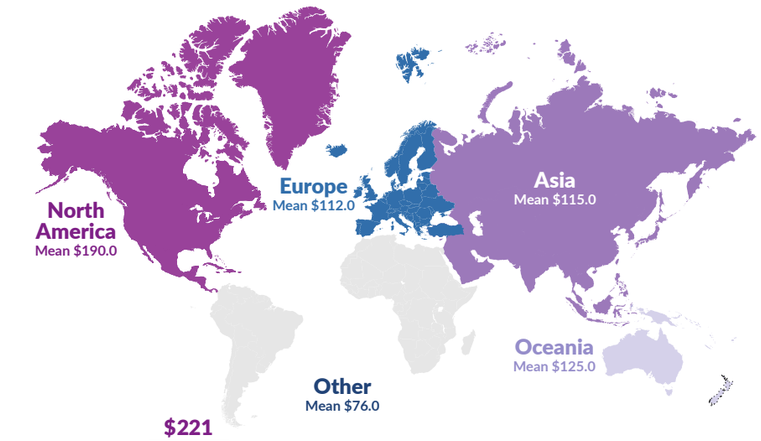
All figures are in thousands of U.S. dollars.

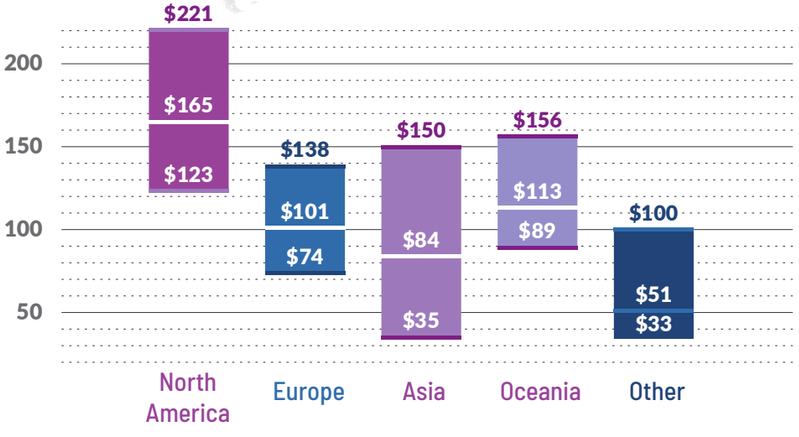
Location

When considering the location of work, average salary breaks down as follows:

Across most roles, respondents based in North America tended to earn more than their counterparts based in Europe, Asia and Oceania. However, it is notable that 50% of global CPOs, internal privacy lawyers and DPO respondents based in Asia and Oceania earned more than their counterparts in Europe. Global CPOs earning the median salary of USD189,000 in Asia earned 20% more than their European colleagues at the median rate. Global CPOs based in North America earned 62% more based on the same measure. The spread of the middle 50% of salaries among CPOs based in Asia (USD153,000) was much larger than the comparative spreads in North America (USD108,000) and Europe (USD81,000).

Global base salaries





AI governance

The following section focuses on those respondents that identified that they have responsibility for AI governance.

Respondents with legal or compliance AI governance responsibilities — those that support compliance within the organization and ensure reporting requirements are fulfilled — earned the highest median salary of USD182,000, compared to the overall median salary,USD158,000.

AI governance base salaries by domain

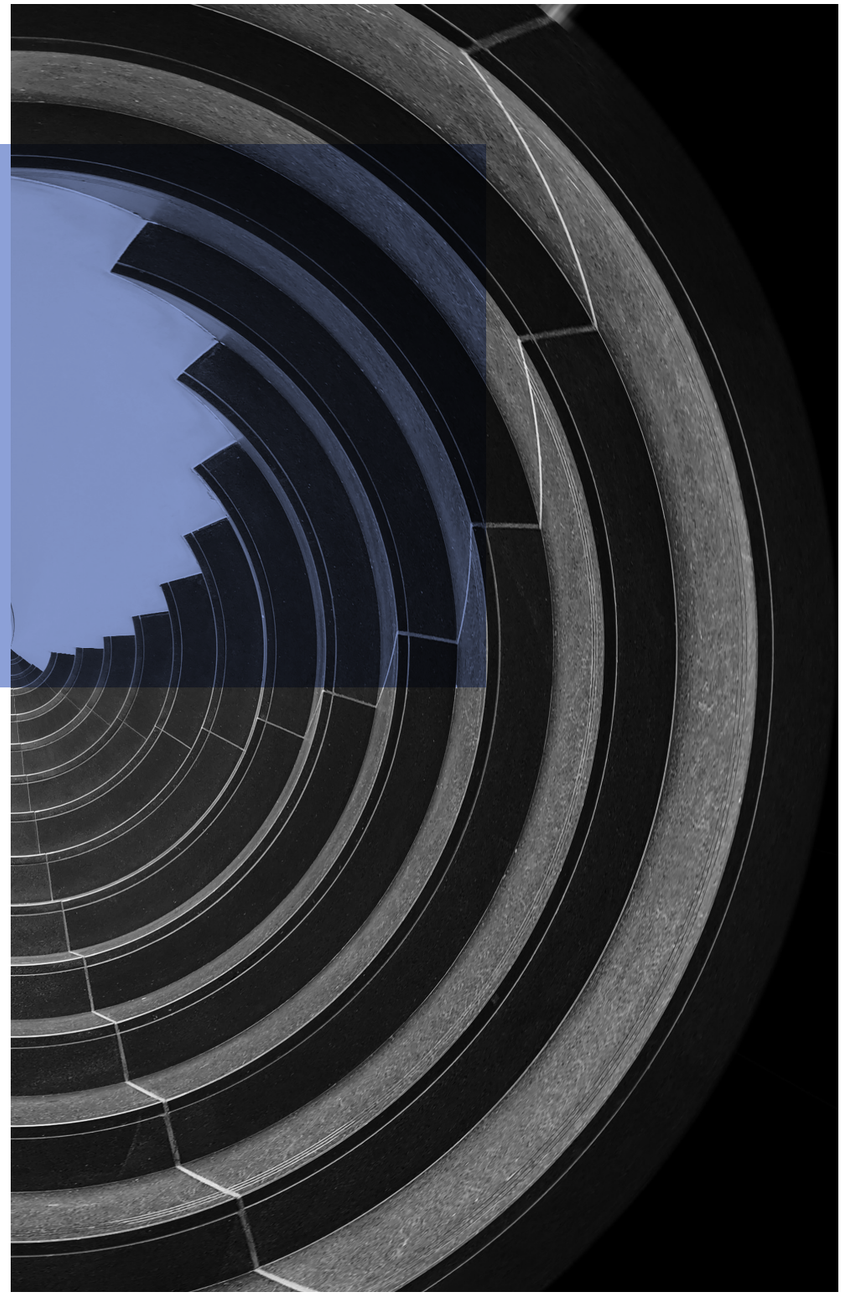
	Legal /compliance	Policy	Governance	Ethics	Risk	Technical	Product	Other AI governance roles
Overall salary	$182.0 ($130.0 - $245.0	$153.0 ($113.0 - $225.0	$158.0 ($122.0 - $206.0)	$117.0 ($80.0 - $137.0)	$150.0 ($103.0 - $185.0)	$175.0 ($145.0 - $216.0)	$155.0 ($89.0 - $205.0)	$158.0 ($96.0 - $219.0)

All figures are in thousands of U.S. dollars.

Selected AI governance base salaries by domain and industry

DOMAIN OF RESPONSIBILITY ANY PRIVACY OR AI GOVERNANCE ROLE	Overall	Technology	Finance	Health care	Retail, media and leisure	Defense, energy, manufacturing and logistics	Government and education	Business services, consulting and legal	Other
Legal/compliance	$182.0 ($130.0 - $245.0)	$205.0 ($141.0 - $260.0)	$159.0 ($116.0 - $215.0)	$187.0 ($125.0 - $297.0)	$198.0 ($158.0 - $250.0)	$189.0 ($147.0 - $245.0)	$142.0 ($134.0 - $220.0)	$167.0 ($125.0 - $240.0)	$126.0 ($86.0 - $217.0)
Policy	$153.0 ($113.0 - $225.0)	$133.0 ($81.0 - $175.0)		$153.0 ($93.0 - $230.0)	$173.0 ($145.0 - $300.0)		$116.0 ($87.0 - $235.0)		
Governance	$158.0 ($122.0 - $206.0)	$139.0 ($117.0 - $205.0)	$160.0 ($139.0 - $200.0)	$149.0 ($137.0 - $210.0)	$164.0 ($117.0 - $210.0)	$170.0 ($134.0 - $213.0)		$127.0 ($117.0 - $176.0)	
Risk	$150.0 ($103.0 - $185.0)	$107.0 ($64.0 - $176.0)	$134.0 ($95.0 - $190.0)	$163.0 ($152.0 - $223.0)			$130.0 ($88.0 - $162.0)		

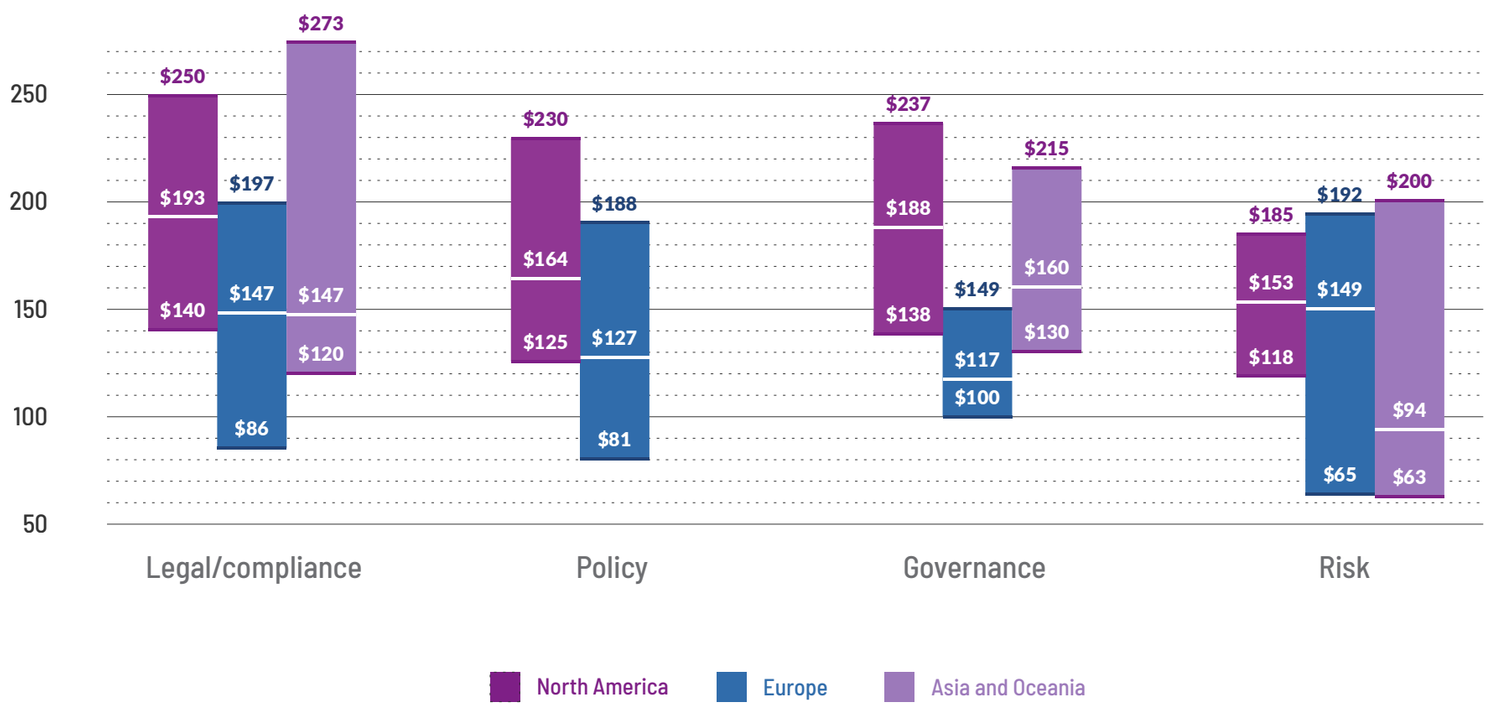
All figures are in thousands of U.S. dollars.



The following trends were noted for those working in AI governance, either as a singular domain or with other responsibilities.

Respondents working across several industries identified their salaries were higher than the overall median salary across all respondents. Those working in the technology sector, either in legal and compliance roles or in technical AI governance roles, earned the highest median salaries relative to other respondents at USD205,000 and USD221,000 respectively.

AI governance base salaries for selected themes by region



All figures are in thousands of U.S. dollars.

Individuals in AI governance roles followed a similar trend — respondents in North America earned more than their counterparts in Europe and Asia. Professionals with legal or compliance AI governance roles were among the highest earners across AI governance roles.

In the majority of cases, the trend holds true for AI governance professionals too: respondents that work for larger organizations get paid more than those that work for smaller organizations. Legal and compliance professionals again enjoyed the highest median salary at USD188,000.

AI governance base salaries by domain and size of organization

	Small — less than $100 M	Medium — $101 M to $999 M	Large — greater than $1 B
Legal/compliance	$170.0 ($123.0 - $260.0)	$166.0 ($106.0 - $225.0)	$188.0 ($136.0 - $250.0)
Policy	$110.0 ($82.0 - $152.)	$180.0 ($113.0 - $270.0)	$179.0 ($138.0 - $225.0)
Governance	$135.0 ($96.0 - $144.0)	$152.0 ($102.0 - $215.0)	$170.0 ($132.0 - $210.0)
Ethics			$117.0 ($95.0 - $159.0)
Risk		$136.0 ($71.0 - $210.0)	$151.0 ($118.0 - $184.0)
Technical			$180.0 ($145.0 - $231.0)
Product			$185.0 ($150.0 - $205.0)
Other AI governance roles	$95.0 ($80.0 - $145.0)	$173.0 ($156.0 - $206.0)	$181.0 ($99.0 - $253.0)

All figures are in thousands of U.S. dollars.

Those working in the technology sector, either in legal and compliance roles or in technical AI governance roles, earned the highest median salaries relative to other respondents at USD205,000 and USD221,000 respectively.

Jobs case study: AI governance lead

This report identifies salary ranges based on the earnings data provided by respondents. Alongside this, it is worth considering the job descriptions and salary ranges of advertised AI governance job vacancies. The following table summarizes relevant information from 100 job openings for roles in AI governance and the corresponding requirements outlined by recruiting organizations. Salary ranges are based on the salaries indicated by those organizations that chose to publicize such data. It should be noted that this is not intended to be an exhaustive list of all compulsory requirements but an illustration of the different types of experience and skills highlighted across sampled job descriptions.

Example titles	Advertised salary ranges	Example experience requirements	Examples of subject matter experience	Examples of soft skills	Examples of qualifications
▫ Director/head of AI governance ▫ AI/ML director ▫ AI transformation lead ▫ AI practice lead ▫ Head of AI enablement ▫ Head of privacy and AI governance ▫ AI governance lead ▫ AI risk lead ▫ Data governance risk lead ▫ Privacy and AI compliance enablement leader ▫ Director of responsible AI	USD120,000 to USD365,000	Ten or more years' experience with progressive technology exposure across areas such as machine learning, natural language processing, deep learning, robotics, product development, business intelligence and digital transformation.	▫ Deep expertise in AI governance principles, ethical AI frameworks and related regulatory compliance, including privacy laws, such as the EU General Data Protection Regulations and the California Consumer Privacy Act, and AI regulation and frameworks, like the EU AI Act and NIST AI Risk Management Framework ▫ Proven track record in leading and managing technical, governance and/or compliance teams with experience in AI governance program leadership within highly regulated industries ▫ Strong understanding of AI/machine learning development and implementation, including experience building products with large language models/AI technologies and proficiency in machine learning tools, platforms and frameworks, such as TensorFlow, PyTorch and AWS AI, and programming languages like Python ▫ Demonstrable experience of working with regulatory agencies, such as the Europea Data Protection Board, Consumer Financial Protection Bureau, the Federal Reserve and state agencies ▫ Expertise in data governance, data privacy and cybersecurity alongside knowledge of data analytics, cloud computing and data management skills, like SQL, ETL processes, and data modeling ▫ Ability to audit AI/ML systems for bias, fairness and compliance with global standards, including designing explainable AI systems and deploying tools to address ethical challenges ▫ Familiarity with ethical AI principles, bias detection, mitigation techniques and privacy-enhancing technologies, such as differential privacy and federated learning ▫ Strong knowledge of regulatory requirements and industry standards related to model risk management with the ability to scale to support other global regulations ▫ Experience leading AI transformation and change management projects, demonstrating the ability to work effectively with cross-functional teams and coordinate risk management activities within complex organizational structures	▫ Strategic leadership: The ability to define and drive AI strategy aligned with business objectives and to drive initiatives from concept to implementation ▫ Team leadership and development: Proven track record of leading, mentoring and developing high-performing, cross-functional teams in complex business environments ▫ Exceptional communication: Excellent written, verbal and presentation skills with the ability to communicate complex issues clearly to senior management, internal/external stakeholders, customers and regulators ▫ Cross-functional collaboration: Demonstrated ability to work effectively with diverse teams, such as engineering, product, compliance, risk, data science, user experience and go-to-market functions to bring complex products to life ▫ Strong business acumen and decision-making: Solid understanding of business principles coupled with strong problem-solving and decision-making skills to evaluate options with speed and a risk-based approach ▫ Executive presence and influence: The ability to recognize and escalate complex or controversial issues, possessing strong interpersonal skills and the capacity to influence stakeholders at all levels ▫ Adaptability and resilience: High tolerance for ambiguity and the ability to thrive in complex environments ▫ Innovation and impact: Proven success in leading large-scale AI or data-driven product initiatives with a focus on measurable business and user impact, including experience building foundational AI systems from the ground up	▫ Bachelor's or master's degree in computer science or engineering ▫ Master's degree in computer science, AI, ML or data science ▫ Advanced degree (JD, master's or Ph.D.) ▫ Certified Information Privacy Professional or similar certifications ▫ Certifications in AI, data privacy or governance, e.g., certified information privacy manager ▫ IAPP AIGP certification, similar certification, or willingness to obtain the certification

Jobs case study: AI governance manager

Example titles	Advertised salary ranges	Example experience requirements	Examples of subject matter experience	Examples of soft skills	Examples of qualifications
▫ AI governance manager ▫ AI program manager ▫ Responsible AI assurance ▫ Compliance and security manager ▫ Responsible AI risk manager ▫ AI automation specialist ▫ AI/machine learning engineer ▫ Generative AI workflow automation developer ▫ Senior counsel - AI technology ▫ Senior AI Risk oversight manager	USD90,000 to USD360,000	Approximately five years of experience	▫ Strong technical foundation in ML/AI with experience in the development of various machine learning techniques, including classical models, transformer-based models, computer vision and large language models, using Python with libraries like PyTorch or TensorFlow ▫ Possess extensive knowledge and experience with generative AI technologies, including LLMs, diffusion models and multi-modal models, such as vision language models ▫ Show a deep understanding of AI/ML development pipelines along with a working knowledge of cloud architectures, AWS, GCP, Azure and DevOps practices ▫ Contribute to or have played a senior role in governance of AI projects, with a strong understanding of responsible, safe, reliable, and robust AI principles ▫ Demonstrate a strong grasp of emerging AI regulations, such as the EU AI Act, legal frameworks for AI governance and the ability to implement legal requirements in AI systems ▫ Possess experience in privacy, security, compliance, and risk management, including knowledge of standards like SOC 2, ISO 42001 and GDPR, with experience in AI risk assessments and cloud security ▫ Understand IP considerations in AI development, including training data rights, model ownership and output licensing ▫ Experience in technical program management, specifically focused on AI/ML initiatives, coupled with an understanding of the challenges in building production-worthy AI systems	▫ Strong leadership and management: Demonstrated progressive experience in management and leadership, including the ability to influence others without direct authority, lead teams and drive change in dynamic environments ▫ Expert project and change management: Proven project management skills with experience leading cross-functional initiatives, coordinating rollouts and implementing change management for new processes, alongside strong problem-solving abilities ▫ Stakeholder management and collaboration: Ability to effectively manage senior and junior stakeholders and client needs, build relationships, facilitate alignment across multiple stakeholders and lead meetings with diverse groups ▫ Strategic thinking and regulatory translation: Capacity to think strategically and creatively, translating complex regulatory concepts into practical implications ▫ Interdepartmental partnership: Experience collaborating with or partnering with legal, compliance, internal audit, enterprise risk or other corporate governance functions ▫ Effective communication and influence: Strong written and verbal communication skills, including the ability to manage time and schedules to meet deadlines and influence through persuasive communication ▫ Business acumen and risk management: Solid business acumen, critical thinking, and decision-making skills, coupled with proven leadership experience in model risk, AI governance or technology risk ▫ Attention to detail and process orientation: Diligent mindfulness, strong technical intuition and experience developing thorough process documentation	▫ A bachelor's degree from an accredited educational institution ▫ An MBA, other advanced degree or equivalent practical experience ▫ Ph.D. in computer science, AI/ML or a related field with a focus on responsible, safe and reliable AI ▫ Certified Information Privacy Professional, Certified AI Ethics Professional, Project Management Professional, Governance and/or Risk and Compliance certifications ▫ Degree in a quantitative or engineering discipline, such as computer science, computational biology, bioinformatics, engineering among others, or equivalent work experience in AI governance

Jobs case study: AI governance analyst

Example titles	Advertised salary ranges	Example experience requirements	Examples of subject matter experience	Examples of soft skills	Examples of qualifications
▫ AI governance analyst ▫ AI and automation governance analyst ▫ Change management analyst ▫ Senior analyst AI governance ▫ Senior AI data analyst ▫ Governance, risk and compliance analyst ▫ AI governance administrator ▫ AI governance and compliance specialist	USD87,000 to USD180,000	Up to five years of experience or equivalent combination of education and/or experience.	▫ Knowledge of AI technologies and their potential ethical and legal implications ▫ An understanding of AI governance principles and industry best practices ▫ Experience developing and implementing governance frameworks ▫ Understanding of responsible AI and/or AI ethics with an understanding of AI technologies and frameworks ▫ Understanding of industry standards and ability to translate emerging global AI regulations into practical, actionable updates ▫ Industry specific governance experience not limited to AI governance ▫ Working within AI governance, risk, compliance or data governance functions in a financially regulated environment ▫ Working with regulatory agencies, such as the EDPB, CFPB, the Federal Reserve and state agencies ▫ Analytics development ▫ Experience with data, decks and dashboards in at least one major business domain ▫ Python, SQL, ETLs, Teradata, Pipelines and Power BI ▫ GRC experience and experience of audit preparations for SOC2, PCI, Health Insurance Portability and Accountability Act and similar standards ▫ Understanding and experience of GDPR, CCPA, the California Privacy Rights Act and other privacy regulations with experience implementing and monitoring compliance processes	▫ Strong commitment to cross-functional collaboration: Able to work effectively with IT, security, sales and engineering to drive the implementation of responsible AI practices, support company success and build customer trust ▫ Self-motivated and organized: Driven individual with a creative approach to project completion ▫ Effective communicator: Excellent written, verbal and interpersonal communication skills with strong communication, presentation and stakeholder management skills ▫ Strong communication: both oral and written and problem-solving skills ▫ Strong analytical and problem-solving skills: An ability to apply these skills to solve a multitude of problems	▫ Bachelor's degree, equivalent relevant work or military experience in a financially regulated environment ▫ Bachelor's or master's degree in law, ethics, information technology, business administration or a related field

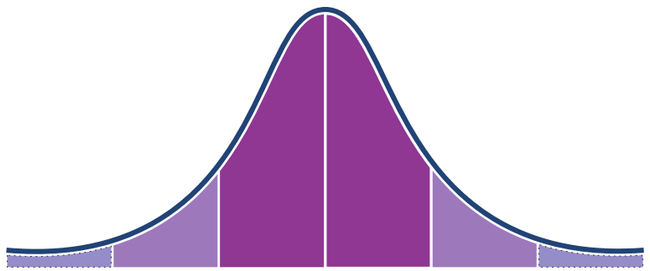
III. Total financial compensation package

What is the overall compensation package?

The overall compensation package is the total financial package an employee receives. By grouping the answers to questions on base salary, hourly pay for those on contracts and renumeration values for additional compensation, we are able to build a view of the average compensation package.

Average total compensation

$202,000



Summary of average total and additional compensation by privacy job title compared to the overall average

	Overall	Global chief privacy officer	Chief privacy officer (country)	Regional privacy officer	Privacy office risk and compliance manager	Internal privacy lawyer	Privacy champion/ guru	Privacy engineer	Cybersecurity professional	Data protection officer	Privacy manager	Privacy analyst	External privacy consultant	External privacy lawyer
Base Salary	**$150.0**	**$226.0**	**$154.0**	**$145.0**	**$130.0**	**$178.0**	**$134.0**	**$155.0**	**$159.0**	**$112.0**	**$89.0**	**$117.0**	**$130.0**	**$196.0**
Overall additional compensation	**$52.0**	**$150.0**	**$36.0**	**$47.0**	**$31.0**	**$62.0**	**$39.0**	**$59.0**	**$24.0**	**$25.0**	**$8.0**	**$52.0**	**$34.0**	**$26.0**
Bonus	*$23.0*	*$62.0*	*$18.0*	*$26.0*	*$15.0*	*$27.0*	*$16.0*	*$30.0*	*$14.0*	*$10.0*	*$4.0*	*$15.0*	*$14.0*	*$20.0*
Stock/equity long-term incentive	*$16.0*	*$67.0*	*$5.0*	*$8.0*	*$9.0*	*$19.0*	*$16.0*	*$12.0*	*$5.0*	*$4.0*	*$0.0*	*$27.0*	*$0.0*	*$0.0*
Cash LTI	*$2.0*	*$3.0*	*$9.0*	*$4.0*	*$1.0*	*$3.0*	*$0.0*	*$0.0*	*$0.0*	*$0.0*	*$0.0*	*$2.0*	*$2.0*	*$0.0*
Cost of living bonus/payment	*$1.0*	*$2.0*	*$0.0*	*$1.0*	*$0.0*	*$0.0*	*$0.0*	*$1.0*	*$2.0*	*$0.0*	*$0.0*	*$0.0*	*$1.0*	*$0.0*
Commission	*$0.0*	*$0.0*	*$0.0*	*$0.0*	*$0.0*	*$0.0*	*$0.0*	*$0.0*	*$0.0*	*$0.0*	*$0.0*	*$0.0*	*$1.0*	*$0.0*
Employer pension	*$4.0*	*$7.0*	*$3.0*	*$4.0*	*$3.0*	*$4.0*	*$6.0*	*$4.0*	*$3.0*	*$4.0*	*$2.0*	*$5.0*	*$5.0*	*$2.0*
Other monetary	*$6.0*	*$9.0*	*$1.0*	*$3.0*	*$2.0*	*$9.0*	*$1.0*	*$12.0*	*$0.0*	*$6.0*	*$1.0*	*$3.0*	*$11.0*	*$3.0*
Total Compensation	**$202.0**	**$376.0**	**$190.0**	**$192.0**	**$161.0**	**$239.0**	**$173.0**	**$214.0**	**$184.0**	**$137.0**	**$97.0**	**$169.0**	**$164.0**	**$222.0**

All figures are in thousands of U.S. dollars.

Global CPOs earn the highest average base salaries at USD226,000 and the highest overall compensation packages, at USD376,000 annually.

Privacy

It's important to consider that the average base salary calculations incorporate figures from contract workers reporting hourly rates, which may overall differ in structure from permanent employee salaries. Additionally, the various additional compensation categories listed may not be applicable to all employees, and individuals should not expect to receive every type of additional compensation presented.

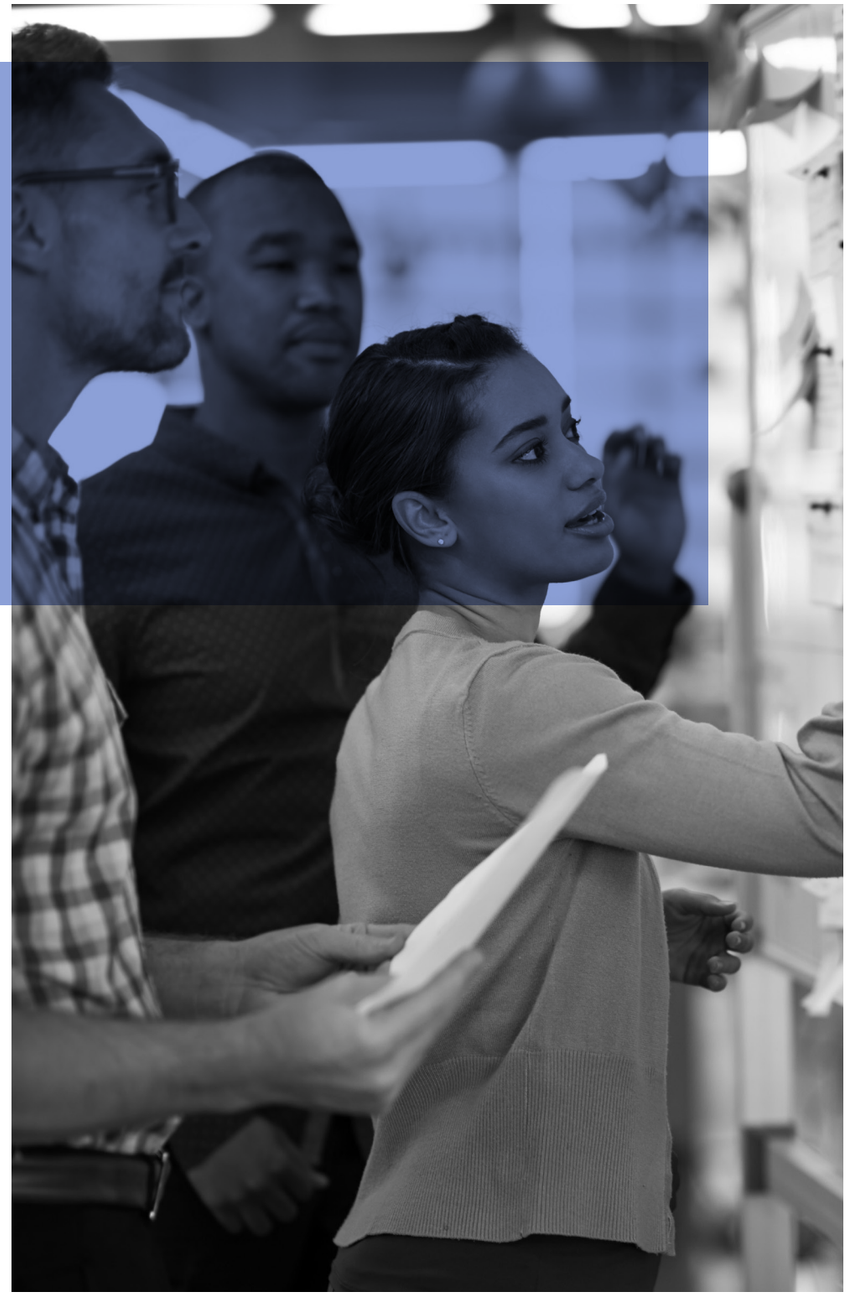
The role-specific breakdowns and information in the table below offer professionals a valuable resource for benchmarking their base salaries and understanding the prevalence of different additional compensation components within the field. This allows for a comparison against specific compensation categories relevant to individual circumstances.

In looking at overall compensation packages, the following can be noted. Global CPOs earn the highest average base salaries at USD226,000 and the highest overall compensation packages, at USD376,000 annually. On average, respondents in this role earned an additional 66% of their average base salaries through additional compensation. In 2023, global CPOs earned an additional 103% of their average base salaries through additional compensation, suggesting that this proportion is lower in 2025.

Summary of average total and additional compensation for AI governance professionals by job title compared to the overall average

	Overall	Legal/ compliance	Policy	Governance	Ethics	Risk	Technical	Product	Other
Base Salary	**$176.0**	**$190.0**	**$169.0**	**$168.0**	**$118.0**	**$145.0**	**$180.0**	**$158.0**	**$168.0**
Overall additional compensation	**$73.0**	**$91.0**	**$45.0**	**$67.0**	**$21.0**	**$45.0**	**$81.0**	**$38.0**	**$44.0**
Bonus	*$32.0*	*$37.0*	*$25.0*	*$32.0*	*$16.0*	*$20.0*	*$25.0*	*$26.0*	*$24.0*
Stock/equity long-term incentive	*$25.0*	*$37.0*	*$10.0*	*$16.0*	*$3.0*	*$9.0*	*$39.0*	*$1.0*	*$12.0*
Cash LTI	*$4.0*	*$3.0*	*$4.0*	*$4.0*	*$0.0*	*$11.0*	*$1.0*	*$3.0*	*$1.0*
Cost of living bonus/payment	*$1.0*	*$2.0*	*$1.0*	*$0.0*	*$0.0*	*$0.0*	*$1.0*	*$0.0*	*$0.0*
Commission	*$0.0*	*$0.0*	*$0.0*	*$0.0*	*$0.0*	*$0.0*	*$4.0*	*$0.0*	*$0.0*
Employer pension	*$4.0*	*$4.0*	*$4.0*	*$5.0*	*$2.0*	*$4.0*	*$3.0*	*$2.0*	*$6.0*
Other monetary	*$7.0*	*$8.0*	*$3.0*	*$12.0*	*$0.0*	*$1.0*	*$8.0*	*$5.0*	*$0.0*
Total Compensation	**$249.0**	**$281.0**	**$214.0**	**$235.0**	**$138.0**	**$190.0**	**$260.0**	**$195.0**	**$212.0**

All figures are in thousands of U.S. dollars.



In external roles, privacy lawyers earn the highest average base salaries at USD196,000 annually and the highest overall compensation packages at USD222,000 annually. On average, respondents in this role earned an additional 26% of average base salary through additional compensation.

Privacy analysts earned average base salaries of USD117,000 with an average of USD52,000 of additional compensation annually. On average, respondents in this role earned 45% of their average base salaries through additional compensation.

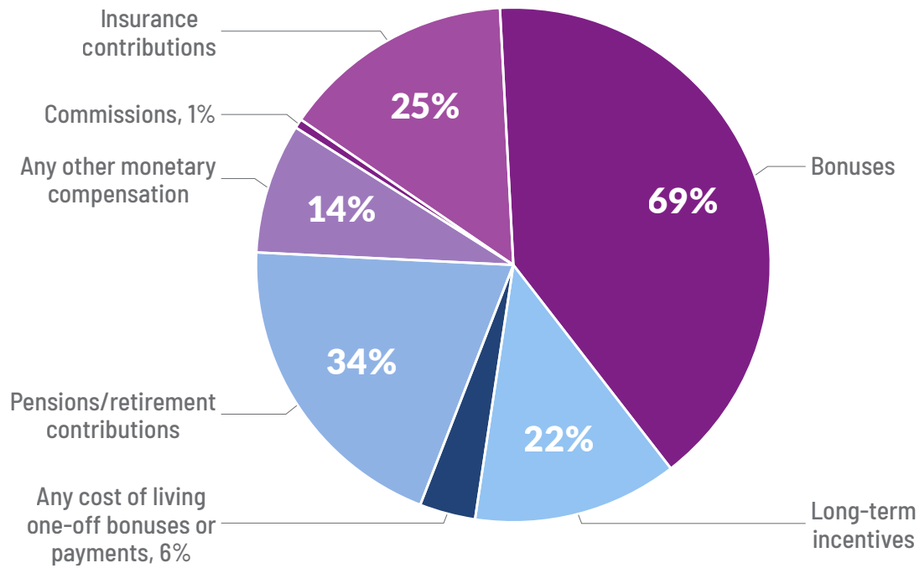
AI governance

Of those respondents with AI governance responsibilities, those respondents working within legal or compliance had the highest total compensation package at USD281,000. These respondents earned 48% of their average base salary through additional compensation. Those respondents working on AI ethics had the smallest total compensation packages with an average base salary of USD118,000, earning an additional 18% of their average base salary through additional compensation.

The tables on the previous pages identify how the specific types of additional compensation available to an employee can vary widely depending on the role, organizational demographics, as well as skills, expertise and experience.

Types of additional compensation received

(% denotes proportion of respondents receiving each type)



Almost 7 in 10 professionals received a bonus, making this the most popular form of additional compensation among respondents. This figure rose to 72% of respondents when only considering those based in North America, but this number fell to 67% of respondents in Europe. The majority of respondents received a bonus based on both personal and company performance (74%), with 11% having a bonus only awarded based on personal performance and 13% having a bonus only awarded based on company performance.

The types of bonuses varied based on organizational size. Those in smaller organizations — either fewer than 100 employees or under USD100 million in annual revenue — were less likely to receive a bonus solely based on company performance. Bonuses with no attached performance metric were more likely to be awarded in smaller organizations.

When breaking this down by role, global CPOs, regional privacy officers and legal or compliance-focused AI governance professionals were most likely to receive a bonus. External privacy consultants were the least likely with only 56% receiving a bonus. Long-term incentives, usually awarded to more senior staff members, were more likely to be awarded to global CPOs — almost half of respondents in this role received this type of renumeration.

The second most popular form of additional compensation was employer pension contributions, received by 3 in 10 respondents. A respondent's location appears to impact the amount of the expected pension contribution. A pension contribution of greater than 8% was only available to 1 in 5 respondents in North America; in the European market, this was amount was received by almost half of respondents. The most generous employer contributions — more than 20% — were again more likely to be received by those working in Europe rather than in North America.

Almost 7 in 10 professionals received a bonus, making this the most popular form of additional compensation among respondents. This figure rose to 72% of respondents when only considering those based in North America, but this number fell to 67% of respondents in Europe.

Average employer pension contribution by region

EMPLOYER PENSION CONTRIBUTION	REGION				
	North America	Europe	Asia	Oceania	Rest of world*
Average	7%	9%	8%	8%	9%

*All figures are in thousands of U.S. dollars. *Note: Small sample size, interpret results with caution.*

IV. Nonfinancial benefits

Nonfinancial benefits play an important role in offering employees a complete compensation package

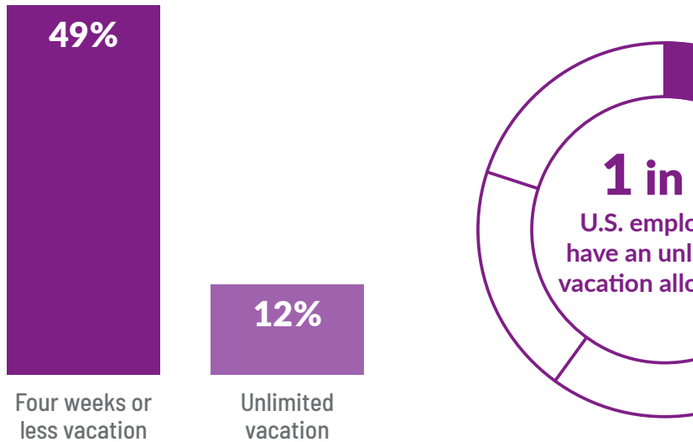
Alongside regular financial compensation, employers often provide nonfinancial compensation in the form of benefits packages. Benefits packages provide employees with additional support and protection, while good benefits packages may have the added bonus of attracting talent, retaining existing employees and rewarding employees who meet or exceed goals. Employees may be more inclined to remain with an organization that offers a strong benefit package; others might be drawn to companies with higher salaries, more extensive vacation time, enhanced retirement plans or greater flexibility in work arrangements. A growing emphasis on work-life balance has prompted organizations to adopt practices like flextime, unlimited vacation and four-day work weeks.

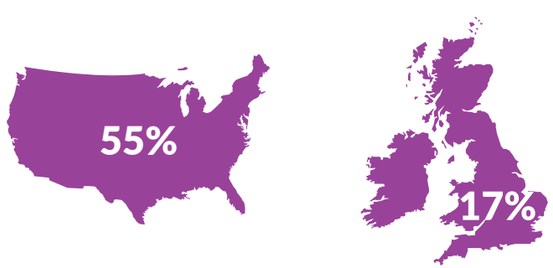
In this year's survey, we explored the nonfinancial benefits enjoyed by respondents.

When considering organization size, respondents working in smaller organizations were given fewer benefits across the key categories included in this survey. Health benefits were enjoyed by at least 88% of those working in medium and large organizations while 77% of those working in small organizations received this benefit.

Vacation allowance plays another key role in how employees are compensated. By region, 76% of Europeans have at least five weeks of vacation allowance. Unlimited vacation allowances were also popular among privacy pros, particularly in North America; this benefit was available to 19% of respondents. This is in stark contrast to the 57% of those in North America with less than four weeks of vacation time, highlighting the divide between vacation allowances available in this market

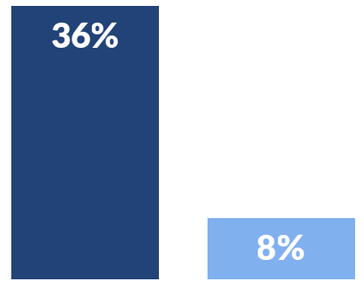
Differences in global vacation allowances

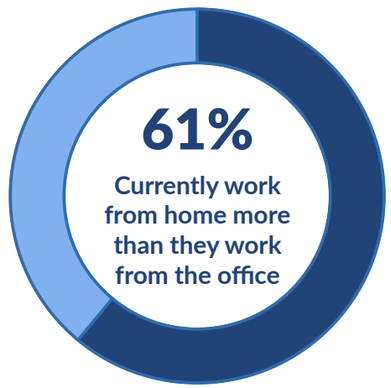


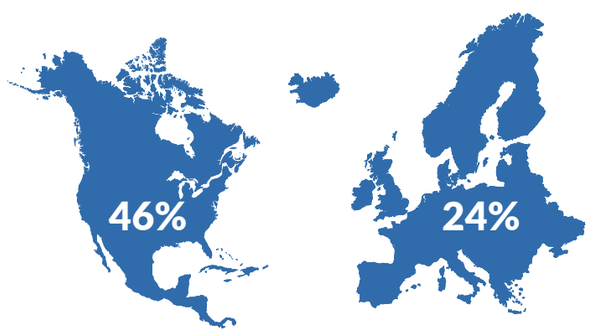


U.S. employees with four weeks or less vacation allowance vs. U.K.

Differences in location of work globally







Currently work fully remote in North America vs. Europe

Third

Full remote work was third most popular job search motivator after pay raise and career progression

V. Impact of certification

Do certifications increase salary?

Further education, training and certification can serve as a significant professional accelerator; they support professionals, expand their knowledge base and, in turn, improve organizational governance. Training and certification can act as an effective differentiator in a crowded job market. Those that complete further education and certification can demonstrate that they have specialized knowledge, show commitment to the field and maintain relevance with amongst constant technological evolution and regulatory changes. In turn, these professionals may be able to obtain a larger compensation package, justify business cases for promotion and secure better career opportunities.

As with the 2023 salary survey, a trend persists in the respondent's highest level of education. An undergraduate degree is the highest level of education for 19% of respondents. A total of 41% of respondents have a law degree. A postgraduate degree, such as a master's or doctorate, was reported as the highest level of education for 1 in 3 respondents. Overall, 95% of respondents reported having some degree-level qualifications.

Respondents continue to add and maintain professional certifications. This year's data identified that at least 77% of surveyed respondents held at least one IAPP certification, while 39% of respondents held multiple IAPP certifications. The pursuit of the Fellow of Information Privacy designation is a unique opportunity for individuals looking to differentiate themselves. A FIP requires a CIPP certification, either a certified information privacy manager or certified information privacy technologist role and three years of experience. The designation was only held by 16% of surveyed respondents — 18% of global CPOs and 6% of surveyed privacy managers hold the designation.

In general, median salary was higher for respondents with any one IAPP qualification. Those holding multiple qualifications yielded further increases in median salary. While these results are not necessarily meant to prove a direct cause-and-effect correlation, it is reasonable to draw a general conclusion that employees with additional qualifications tend to be more valuable to their organizations.

Base salary by number of qualifications held

	No IAPP qualification	Any one IAPP qualification	Multiple IAPP qualifications
Global chief privacy officer	$200.0 ($112.0 - $250.0)	$202.0 ($150.0 - $280.0)	$261.0 ($190.0 - $300.0)
Chief privacy officer (country)	$131.0 ($95.0 - $180.0)	$148.0 ($105.0 - $196.0)	$168.0 ($160.0 - $238.0)
Regional privacy officer	$151.0 ($73.0 - $220.0)	$127.0 ($90.0 - $161.0)	$175.0 ($127.0 - $223.0)
Privacy office risk and compliance manager	$116.0 ($80.0 - $154.0)	$117.0 ($79.0 - $170.0)	$160.0 ($116.0 - $190.0)
Internal privacy lawyer	$151.0 ($116.0 - $195.0)	$173.0 ($114.0 - $225.0)	$200.0 ($165.0 - $235.0)
Privacy champion/guru	$108.0 ($59.0 - $137.0)	$142.0 ($137.0 - $163.0)	
Privacy engineer	$136.0 ($95.0 - $176.0)	$165.0 ($110.0 - $265.0)	
Cybersecurity professional	$156.0 ($121.0 - $190.0)	$149.0 ($127.0 - $184.0)	
Data protection officer	$95.0 ($67.0 - $140.0)	$110.0 ($82.0 - $152.0)	$116.0 ($91.0 - $159.0)
Privacy manager	$115.0 ($82.0 - $145.0)	$92.0 ($68.0 - $124.0)	$150.0 ($102.0 - $164.0)
Privacy analyst	$92.0 ($68.0 - $107.0)	$91.0 ($56.0 - $105.0)	$107.0 ($73.0 - $130.0)
External privacy consultant	$121.0 ($51.0 - $138.0)	$121.0 ($81.0 - $196.0)	$127.0 ($88.0 - $186.0)
External privacy lawyer	$183.0 ($119.0 - $227.0)	$186.0 ($135.0 - $270.0)	$190.0 ($140.0 - $310.0)

All figures are in thousands of U.S. dollars.

This year's data identified that at least 77% of surveyed respondents held at least one IAPP certification, while 39% of respondents held multiple IAPP certifications.

VI. Movers and shakers

To leave or not to leave, that is the question.

The relationship between how content employees are in their current roles, the key drivers that entice individuals to seek new opportunities and the prevalence of active job hunting can reveal several insights into the dynamics at play in the workforce. Understanding this relationship is key to organizations proactively addressing dissatisfaction and the ability to tailor their employee value proposition to align with what truly motivates the workforce.

Employee motivation, the crucial skill of boosting and sustaining high morale, is often central to an organization's achievements. Without it, decreased engagement, commitment, and job performance can hinder organizational goals and diminish the potential for a thriving work environment. This year's survey underscores compensation as a significant driver of employee satisfaction. Fair and competitive pay demonstrates an organization's value of its workforce, directly influencing morale and the desire to excel. Beyond basic satisfaction, attractive compensation packages can enhance recruitment efforts, improve employee retention rates and foster a more dedicated and productive team — ultimately contributing to a more successful and positive workplace.

As with prior years, this year’s survey shows that compensation and career development are critical factors in employees’ satisfaction.

Job satisfaction was generally high among respondents, with 81% rating their satisfaction in their current role above six out of ten, including 31% who indicated the highest levels of satisfaction, scoring between nine and ten.

AI governance ethics professionals and global CPOs were happiest in their role with 54% and 41% respectively reporting a satisfaction level between nine and ten. This included two in five AI governance ethics professionals and one in five global CPOs that gave a perfect score for job satisfaction. Conversely, respondents with the job titles privacy champion/guru and AI governance product professionals were the least satisfied in their roles, with 32% and 33% respectively selecting a score between zero and five.

The average and median salary of those that reported the highest satisfaction were higher than those that reported that they were not as satisfied with their role. However, with overlapping salary bands, the direct connection between higher job satisfaction and salary is not clear.

SATISFACTION	Frequency
0-5	19%
6-8	50%
9-10	31%

Impact of job satisfaction on base salary

	JOB SATISFACTION		
	0-5	6-8	9-10
Median (Q1 to Q3)	$134.0 ($89.0 - $188.0)	$138.0 ($94.0 - $190.0)	$141.0 ($96.0 - $204.0)
Mean	$142.0	$164.0	$161.0

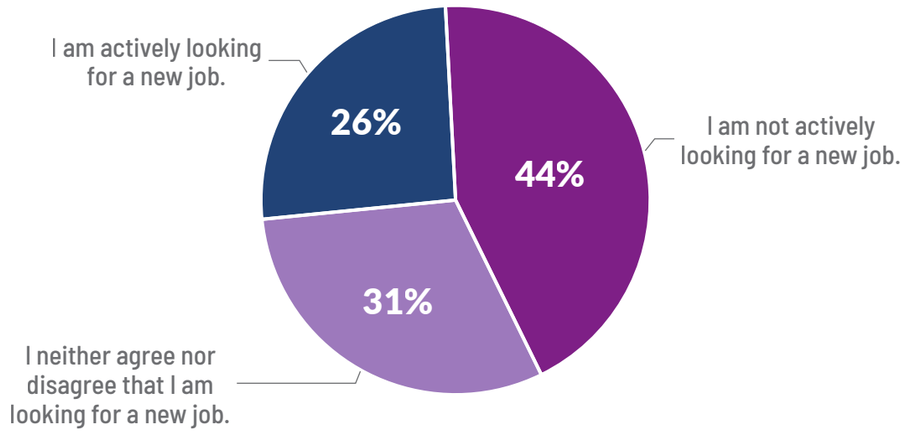
All figures are in thousands of U.S. dollars.



Top three motivating factors causing respondents to seek new jobs



The extent to which respondents are actively looking for a new job



Instead, we can consider the factors identified by respondents that would cause them to move jobs.

The combination of pay raise and career progression was chosen by almost half of all respondents, highlighting the importance of these factors. One in four respondents that chose both pay rise and career progression also selected the possibility of an improved role with responsibilities as the third factor that would motivate them to move jobs. A further one in four chose the opportunity for fully remote work as the third motivating factor alongside pay rise and career progression. In terms of retention, employers and managers should consider the extent to which each of these factors are being met for team members in their current roles.

We can also consider the extent to which respondents are actively seeking a new role.

As the pie chart on the left shows, one in four respondents actively seeking a new role, it's clear that a significant proportion of the workforce are seeking a new role. Somewhat unsurprisingly, 67% of those who said that they were not satisfied with their current role also identified that they are actively looking for a new role. The active job-seeking efforts of one in four respondents highlight the intensity of the job market and the level of competition applicants may face for any given role.

VII. What's next?

How can organizations and professionals respond to the findings of this report?

With financial wellbeing of employees in flux and ongoing pressures on salary budgets and onward compensation, organizations and professionals may be left considering how they can respond. For organizations setting accurate pay can be the enable its compensation strategy to support overall business objectives. For professionals, reviewing pay offers to opportunity to question whether pay is fair, prepare for salary negotiation discussions, support future career planning, and understand the market more broadly. This section highlights potential actions that individuals and organizations may consider taking.

Personal



Compare your positioning within a salary band by looking at adjusted salary penetration.

Review your salary against the most relevant pay band, taking into account the lower bound (Q1 or the 25th percentile value) and the higher bound (Q3 or the 75th percentile value). Use the following formula:

$$Adjusted\ salary\ penetration = \frac{(Your\ salary - Q1)}{(Q3 - Q1)}$$

The result is expressed as a percentage, showing where your salary falls within the selected salary range. Please note that only limited conclusions should be drawn from these results as these ranges are based on the 75% and 25% percentiles rather than precise boundaries.



Consider the impact of certifications.

Identify certifications relevant to your role that align with your goals, consider industry demand and, potentially most importantly, align with personal development interests. Evaluate the costs of undertaking additional certifications against the benefits, considering both financial costs and time commitments. Consider discussing the needs for additional certifications with internal and external stakeholders who can share insights into the impact of pursuing additional qualifications.



Compare your likelihood of searching for a new role vs. peers to give an indication of job search intensity.

Data in this report identified that one in four respondents are actively seeking a new role and 67% of those who said that they were not satisfied with their current role also identified that they are actively looking for a new role. Considering the likely competition faced when applying and interviewing for a role is a crucial part of strategically positioning yourself to obtain the best role. Whilst it may not be possible to gather formal metrics accurately on job search intensity, industry reports, professional communities and popularity of job adverts can give some insight into potential volume of competition.



Consider integrating salary band information from this report and other sources into negotiations.

Salary reports can provide transparency over compensation in the market and play a vital role in establishing a realistic salary range for a role. The specific job title, industry, location, company size and experience, amongst many other factors, can all impact the salary ranges available. However, data can be a crucial tool in providing quantitative evidence to support requests for compensation commensurate with the role. It's worth noting that salary and other financial compensation is only one component of total compensation and therefore important to also weigh up nonfinancial benefits on offer too.



Identify where a promotion, change in role, increases in seniority and/or increase in tenure may further salary prospects.

Whilst a change in role may be likely to lead to an increase in compensation, it's important to consider whether existing roles may also provide further opportunities. The data supports this with 80% of respondents securing a rise in base salary over the previous 12 months.



Compare the salary survey data against job advertisements without salary information to estimate potential compensation.

The salary ranges included in this report may provide a useful benchmark for roles that do not advertise any pay information. The data included in this report can form a useful benchmark, although care should be taken as the data includes submissions from those new in role and those that have much longer tenures.

Salary reports can provide transparency over compensation in the market and play a vital role in establishing a realistic salary range for a role. The specific job title, industry, location, company size and experience, amongst many other factors, can all impact the salary ranges available.



Organizational

Benchmark your organization's salary bands vs. those in the report.

Reviewing salary report data can be a useful tool in identifying whether existing internal pay structures are fit for purpose. This can support organizations in maintaining salary parity with competitors in order to attract and retain talent, support internal equity and consistency in pay, avoid under/overpaying for roles, meeting legal requirements around pay and maintaining resilience in workforce planning.

Compare this to desired talent acquisition and retention strategies.

A core part of future workforce planning is likely the need to understand overall strategy, growth plans and corresponding future skill requirements. These likely impact current workforce planning and succession management. For example, an organization that is seeking to invest heavily in AI development may need a corresponding AI governance function, for which it may be important to offer comparatively leading salaries in order to attract top talent. Conversely organizations may choose to follow a lagging pay strategy should future plans include a more streamlined second line function.

Identify whether pay scale remediation is required and work with HR to amend.

A pay scale remediation exercise, either retroactive or forward looking, may be required to address pay fairness and issues of equity. Should digital governance professionals suspect this to be the case within their teams it may be pertinent to work with HR to identify discrepancies, conduct further internal and external benchmarking activities, and implement changes as needed.

Understand how to leverage existing expertise and workforce for broader digital governance domains and approach hiring and training staff.

Redeploying and using existing expertise within organizations may likely form a critical part of how organizations respond to digital governance challenges. Organizations may be able to achieve time and cost savings by doing so, with the opportunity to leverage existing skills and knowledge whilst offering employees the opportunity to learn new skills possibly benefiting all involved parties.

Contacts

Connect with the team

Saz Kanthasamy
Principal Researcher,
Privacy Management, IAPP
skanthasamy@iapp.org

Joe Jones
Research and Insights
Director, IAPP
jjones@iapp.org

Follow the IAPP on social media

Published August 2025.

IAPP disclaims all warranties, expressed or implied, with respect to the contents of this document, including any warranties of accuracy, merchantability, or fitness for a particular purpose. Nothing herein should be construed as legal advice.

© 2025 IAPP. All rights reserved.