2022 DATA PRIVACY JOBS REPORT

Also Included:

2023 State of the Privacy Job Market

CONTENTS

LETTER FROM TRU'S CEO

Privacy is having a moment — one that's showing no signs of slowing down.

In 12 years of running TRU Staffing Partners, this is the highest demand for data privacy and protection professionals I've ever seen.

Growing concern over data privacy compliance in an increasingly complex regulatory environment is colliding with corporate awareness of the opportunity to build consumer trust and brand credibility through strategic data privacy program implementation. Happening against the backdrop of a global pandemic that forced a massive recalibration of human capital management, retention, and acquisition, the job market for data privacy shines like a beacon of opportunity, beckoning ambitious legal and technology professionals to join one of the fastest-growing and highest-paid professional ecosystems in the world.

Privacy is now everyone's problem (and opportunity). COVID-19 caused a sudden, seismic shift to virtual employment. Overnight, companies created digital employee cultures and rapidly adopted online customer acquisition strategies, which inherently raised data-usage questions that only privacy professionals were equipped to answer. But as digital privacy became important in social consciousness (specifically hyperawareness and miseducation surrounding privacy rights related to healthcare data like vaccine status), regulatory risk shifted to brand ambassadorship in corporate consciousness.

Businesses of all sizes need and want experienced data privacy talent right now; however, privacy staffing is not one-size-fits-all. Every organization is in a unique state of data privacy program maturity — from needing ground-zero executive leadership to building robust privacy engineering teams. Each company has different regulatory requirements. Access to successful, proven people and approaches to building, growing, or maintaining novice or highly complex data privacy teams is a mission-critical need — and often elusive.

"...this is the highest demand for data privacy and protection professionals I've ever seen."

This compendium includes TRU's key takeaways from serving the data privacy community for more than a decade, coupled with our proven strategies to help increase successful attraction and acquisition of data privacy talent — with or without the help of talent agents like TRU.

It's time to up-level job descriptions (page 7), clearly (re)define your approach to interviewing talent (page 8), map your program maturation model (page 14), speak to technology integration (page 18), and most importantly, be able to articulate all of this to prospective candidates from entry-level to seasoned executive.

Privacy pros view the hiring process as a gauge of a company's commitment to and valuation of privacy, so it's important to send signals that show candidates they'll be valued (page 16).

For both hiring managers and job seekers, it's an exciting time for the privacy profession, and TRU is proud to represent so many in this community!

Jared Coseglia
Founder & CEO
TRU Staffing Partners

30% YEAR-OVER-YEAR INCREASE IN AVAILABLE PRIVACY ROLES

> ***"It's not just a shortage of people — it's also a struggle to attract the right people."***
>
> **— Rachael Haher, CIPM**
> VP of Business Development
> & Account Management

ROLE DEFINITIONS MATTER NOW MORE THAN EVER

In 2021 and 2020, there was a 30% year-over-year increase in available privacy roles. With the trend expected to continue, if not accelerate, through 2022 and beyond, role definitions are a critical tool for attracting truly qualified candidates.

"Everyone is clamoring over a shortage of talent in privacy, which is real," says Rachael Haher, Vice President, Business Development and Account Management at TRU Staffing Partners. "But it's not just a shortage of people — it's also a struggle to attract the right people because of a misalignment of titling, reporting structure, compensation, and job requirements."

In other fields — ediscovery, for example — things are simpler. An "analyst" is a data processor. A "project manager" is a case manager. There's general consensus on leveling and compensation ranges. Privacy has yet to fully codify industry wide.

"The same title in one organization can mean something completely different somewhere else, depending on the size of the privacy program," says Haher. "Same with compensation. Based on title, a privacy job posting might at a glance look the same as another, but the actual responsibilities and compensation are totally different. Things just aren't standardized yet."

A thoughtfully crafted data privacy job description that takes the mystery out of the most common questions job seekers look to have answered before expressing interest in employment within a corporate privacy program can be the key to capturing the right candidate's attention.

This has been further complicated in recent years by radical alterations in broader job market trends related to post-pandemic virtual employment adoption and economic inflation. "Even if you do find the right people, do you find them fast enough, and can you offer something uniquely competitive to entice them to choose your organization?" adds Haher.

There can be a temptation to go generic on job descriptions in hopes of attracting more candidates. This usually backfires. Especially in a specialized industry like privacy, a clearly articulated program vision coupled with detailed responsibility specificity is the name of the game. Answers to these questions can help create a job description that speaks directly to the typical privacy job seeker.

NEED HELP CREATING A PRIVACY JOB DESCRIPTION? SCAN THIS QR CODE TO GET ACCESS TO TRU'S PROPRIETARY PRIVACY JOB DESCRIPTION BUILDER.

ANSWERING THESE CRITICAL QUESTIONS BEFORE YOU START YOUR INTERVIEW PROCESS & WRITE YOUR JOB DESCRIPTION WILL ENSURE GREATER SUCCESS

Q&A BEFORE YOU Q&A

EXTERNAL PARTNERS

"Do you use outside counsel & consulting firms for privacy? If so, for what functions?"

Experience managing third-party resources can be a mission-critical skill, and one that people who are good at like to brag about.

REPORTING STRUCTURE

"To whom does this role report? To whom does that role report? Is privacy under legal? IT? The COO? Will this role have direct reports? If so, who? If not now, when? What other dotted-line reporting will this role have?"

These reporting questions are specifically critical for capturing the attention of CPOs, most of whom have strong opinions about what the reporting structure needs to be for them to make a move.

TITLE

"Is the title specific, level-appropriate, and recognizable in the current market? Are you consciously asking someone to take a title downgrade to fit into your current company leveling?"

Forget about losing leverage for future job moves by taking a title lesser than a current one. Privacy pros are much more concerned with their title and leveling, giving them the gravitas needed to be successful in their new role.

PANDEMIC CLARITY

"Is working remotely permitted? Are there vaccination requirements? If hybrid, are there set in-office days? Rotating schedule?"

Do not wait until you start talking to talent to unpack all these policies! What a waste of time if you're not aligned. Spell out how your company's employment policies have been altered because of COVID-19, and weed out candidates who won't embrace your rules.

PRIVACY RESPONSIBILITIES

"On a percentage basis, how will this role divide their time across these areas at the time of hire: Programmatic/operational, legal counsel, policy writing, risk assessment, data strategy, information governance, compliance, technology, product development/management, privacy engineering, contracts/third-party management?"

We encourage hiring managers to break down the role in percentages, sometimes visually, so job seekers see where the impact on the enterprise or on products will be made on day one, and what a future state looks like in terms of adjusted priorities over time. Check out TRU's proprietary data privacy job application, where you can see the kinds of questions we ask candidates.

MISSION

"What is the company's mission? How does that mission connect to the privacy program?"

Privacy job seekers are mission-driven professionals, and the more experienced, the more their employer's enriched connection of privacy to business agenda matters.

VERTICALS

"How important is expertise in specific industry verticals?"

If important, say so. If it's not important, say so. Too often people do not apply to banks, for example, because they assume experience in financial services is a prerequisite.

TEAM SIZE/SCOPE

"How many members are on the privacy team? How many combined years of experience does your team have in data privacy?"

Who people will work with, who their leaders will be, and whether they'll have an opportunity for mentorship, are key reasons why people leave one job for another. JJob seekers have strong opinions about the size of the team with which they would best fit. Spell it out.

REGULATORY RESPONSIBILITIES

"What percentage of time will this role interact with the following types of data: Employee, consumer, patient, and third-party? What is the geographic scope of data? Which privacy laws apply to your company?"

Privacy pros, especially legal ones, want to know the scope of your compliance requirements so they can point explicitly to their experience with each. This is especially useful in attracting talent when the governing laws are not as common as, say, GDPR or CCPA.

TECHNOLOGY TOOLS

"What enterprise tool stacks will this role interact with? What tools are you currently using or planning to use for privacy functions such as activity monitoring, assessment management, data discovery and mapping, data subject access request automation, pseudonymity, incident response, privacy information management, and website scanning?"

More detail here creates industry-exclusive keywords that help align resume search automation.

TO COUNSEL OR NOT TO COUNSEL

"Is a J.D. required for the role? Must they be barred or is it just nice to have the credentialing? Will this person be expected to give legal counsel?"

Often, companies want lawyers in privacy roles, but that does not always mean they are part of the office of the General Counsel or that they are expected to give legal advice. Be clear on how the company uses and values their legal degree in this particular role, if required.

CURRENT/FUTURE STATE

"How mature is your privacy program? Will you be building out a privacy program, running a privacy program, or elevating an established program?"

For everything you need to know about the state of privacy programs, turn to page 14.

FAST, FLEXIBLE, & FINANCIALLY ALIGNED

THE 3 Fs

SPEED MATTERS

In 2019, the average timeline from sending a resume to getting an offer for a midmarket, full-time privacy candidate was three to six weeks. For executives, directors, and CPOs, that timeline was three to six months. In 2021, the timetable for hiring a program manager, analyst, specialist, or engineer truncated to a mere eight business days. For executives, the timetables shrank to a rapid three to six weeks. The midlevel hiring timetable extended slightly in Q1 2022 (from 8 days to 12) and Q2 of 2022 (from 12 days to about 20). While speed of hire has slowed with traditional market ebbs & flows (summer interviews always take longer than spring or fall), the pace at which hiring occurs remains dynamically faster than before the pandemic. 79% of midmarket job orders are still filled by TRU in the first 30 days.

Speed of hire will never be the same — companies that do not adjust will lose talent to competing offers.

Thanks to adoption of virtual interviewing (100% of first-round interviews in 2021 and 2022 were virtual, and 95% of all subsequent rounds were as well), the speed of hire will never be the same. Companies that do not adjust will lose talent to competing offers: Currently, privacy job seekers had an average of three, but a minimum of two, competing offers to choose from (including counteroffers from current employers).

REMOTE MATTERS

Work-from-home flexibility has become a bargaining chip. In high-demand spaces like data privacy, allowing employees to work remotely can turn unfilled roles into a thriving privacy program.

"Bottom line: Adopting a remote culture increases your talent pool and retains your existing employees," says Jess Barre, Vice President of Recruitment and Account Management at TRU Staffing Partners. 77% of TRU's placements in 2021 were fully remote work-from-home opportunities. In parts of the country where there are a smaller number of privacy professionals, requiring on-site work greatly limits hiring managers. "Not only are in-office job requisitions limited to local talent, but those local talent pools are also now interviewing for a corpus of jobs all over the world that offer remote employment that was not available to them prior to the pandemic. 88% of jobs filled by TRU in 2022 were either fully remote or hybrid positions."

Is on-site work ever the right way to go? Certainly. For net-new team positions or in cases where organizations are looking to hire a privacy leader, being visible to executives/stakeholders can be important. "When there's a need to win people over, face-to-face visibility usually helps," says Barre. "If you want a seat at the table, sometimes you have to go to the table — wherever that is."

Despite many companies wanting in-office representation from data privacy hires, the investment in relocating talent is astronomically low. The amount of privacy pros being relocated is down from 27% in 2014 to 3% in 2021. That cost savings is going right back into increased labor spend.

COMPENSATION MATTERS

The average increase of base compensation at the point of hire in 2021 for midmarket privacy professionals was 22%. So someone making $110K in salary is now likely making around $141K base compensation. Add inflationary awareness to the job seekers' self-valuation and companies can expect data privacy professionals to command — and get — upwards of 25-30% increases from their current compensation in 2022.

COMPENSATION METRICS

TRU rarely releases salary information, but when we do, our data is based on offers candidates were extended and had accepted. This data is not a survey of what these titled employees are making, but rather what companies have been willing to offer at the point of hire. Despite frequent role definition disparity across the industry (see page 7), the titles below best describe trending leveling and hiring practices. Additionally, all industry verticals are not listed here, but compensation metrics generally fit into these three broad categories:

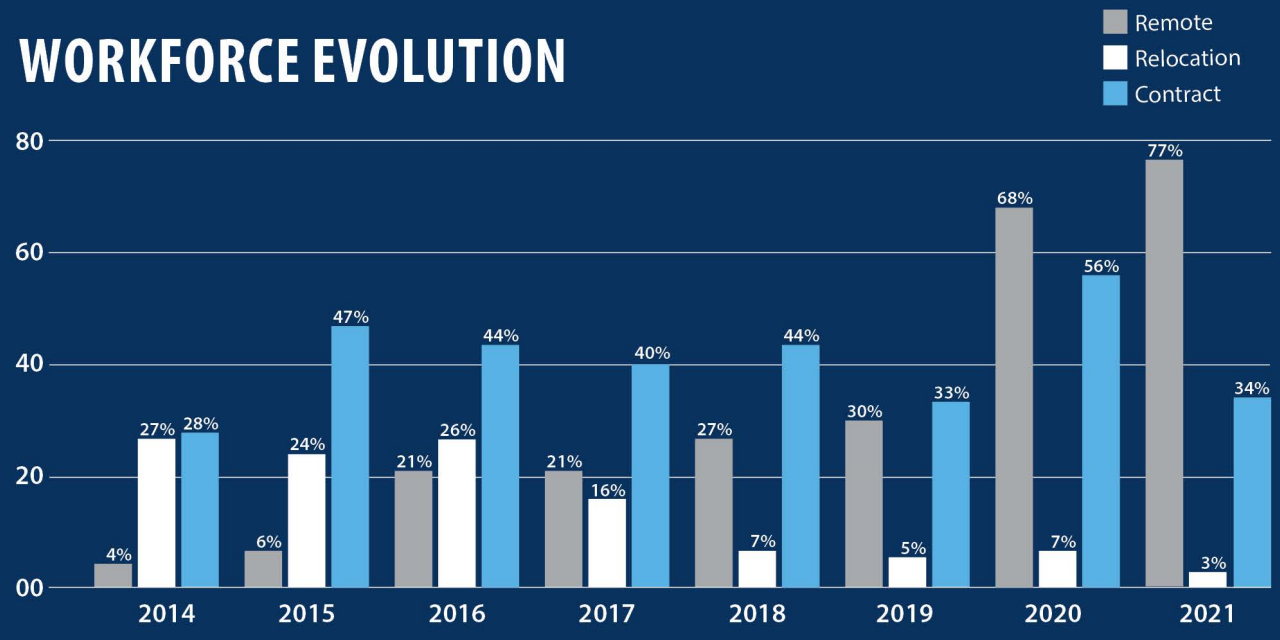
BASE SALARY IS LISTED WITHOUT PARENTHETICALS; TOTAL COMPENSATION IS INDICATED IN PARENTHESES.

	BIG TECH	FINANCIAL/ HEALTHCARE/ HEALTHCARE TECH	TELECOMM/ RETAIL/ ENTERTAINMENT
Entry Level	$60K - 85K ($70K - 95K)	$60K - 85K ($70K - 95K)	$60K - 75K ($70K - 85K)
Privacy Analyst/ Specialist	$90K - 140K ($90K -165K)	$90K - 140K ($90K - 165K)	$90K - 130K ($90K - 150K)
Privacy Program/ Project Manager	$140K - 180K ($165K - 250K)	$130K - 160K ($145K - 175K)	$130K - 160K ($145K - 175K)
Privacy Sr. Manager/ Consultant	$175K - 200K ($200K - 250K)	$140K - 170K ($160K - 190K)	$140K - 160K ($160K - 180K)
Privacy Directors/ SMEs	$225K - 300K ($300K - 400K)	$200K - 260K ($230K - 320K)	$200K - 250K ($230K - 300K)
Privacy Engineer	$175K - 300K ($225K - 460K)	$150K - 235K ($175K - 360K)	$150K - 205K ($175K - 325K)
Privacy Counsel	$225K - 325K ($275K - 450K)	$200K - 300K ($250K - 400K)	$175K - 320K ($200K - 400K)
CPOs/ Business Unit Privacy Leads	$265K - 465K ($325K - 1.5MM)	$235K - 425K ($275K - 800K)	$225K - 315K ($275K - 600K)

All data reflected above is in USD and reflects US compensation ranges.
TRU can consult on global geographic compensation adjustments upon request.

HOW HAS THE PANDEMIC AFFECTED THE JOB MARKET?

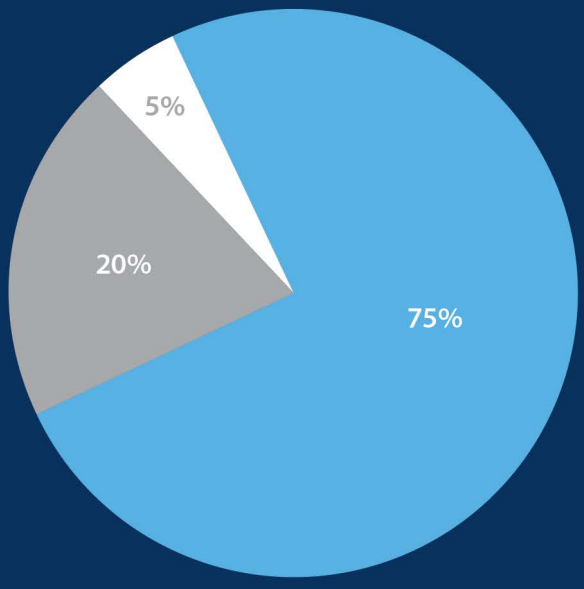
WORKFORCE EVOLUTION



TRU TRENDS

- **77%** new hires are now remote
- **40%** increase in job orders
- Candidates entertained an average of **3** offers at the time of acceptance
- **100%** of first-round interviews were virtual in 2021 and 2022
- **88%** of all roles filled by TRU in 2022 were either fully remote or hybrid positions
- **22%** base compensation increase for midmarket professionals at point of hire in 2021

WHERE ARE THE JOBS IN PRIVACY?



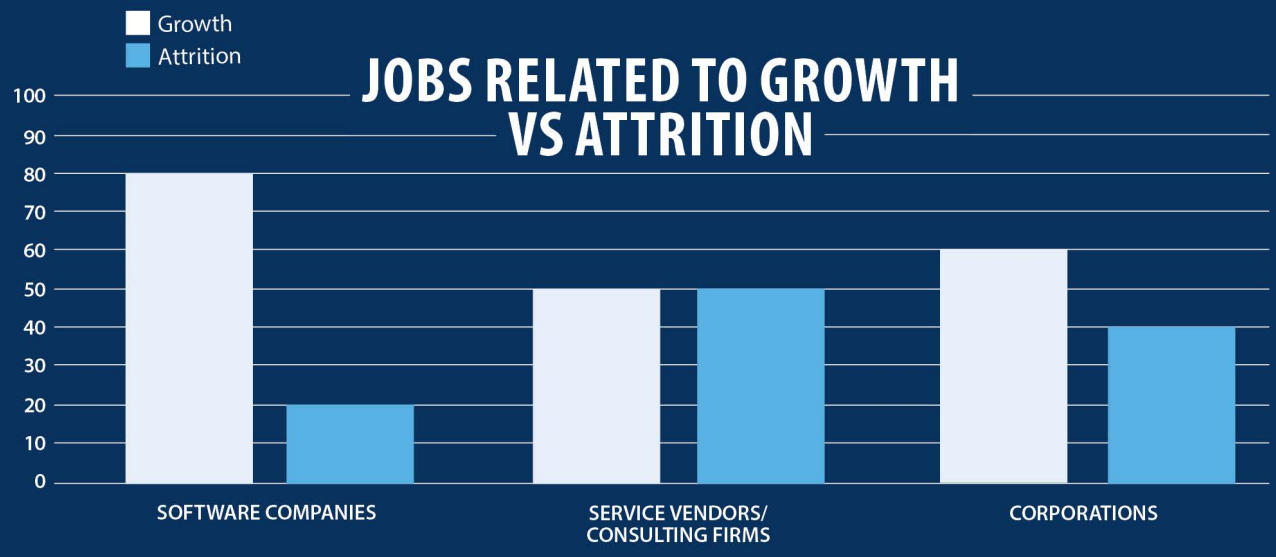
SPEED OF HIRE: BEFORE & AFTER

2019 TIME TO HIRE	2021 TIME TO HIRE	2022 TIME TO HIRE
MIDMARKET, NON-CONTRACT	MIDMARKET, NON-CONTRACT	MIDMARKET, NON-CONTRACT
3-6 WEEKS	8-12 DAYS	20-30 DAYS
CONTRACT	CONTRACT	CONTRACT
2 WEEKS	48-72 HOURS	1 WEEK
EXECUTIVE	EXECUTIVE	EXECUTIVE
3-6 MONTHS	3-6 WEEKS	4-8 WEEKS

TOP 5 MOTIVATIONS OF JOB SEEKERS IN 2021

1. Working remotely/hybrid
2. Mentorship/new leader
3. $$$$$$$
4. Upskilling
5. Diversity, equity, & inclusion

JOBS RELATED TO GROWTH VS ATTRITION



PITCHING YOUR PRIVACY PROGRAM

To fill privacy roles with the right candidates, organizations can map the current and future maturity models of their privacy program to articulate these models to job seekers. TRU has found there are four easy ways to categorize and express maturity states of privacy programs on interviews.

BUILDER

If you are a small core team that is often supplemented with contractors, fractional internal resources, reliance on consulting firms and outside counsel, and/or in early stages of hiring, you are the **BUILDER**. An entrepreneurial spirit, the ability to wear multiple hats, the ability to explain and evangelize privacy across departments, and a broad knowledge base around privacy legislation are required. Most departments that are Builders are highly advisory in nature.

GROWER

As a privacy program matures, priorities become more operational and technical, more time is spent on strategic execution, and less time is spent on establishing buy-in. Your program will be in the **GROWER** stage when it begins to move from an advisory function to an accountable one. Roles begin to compartmentalize responsibilities, and staffers are valued for being privacy specialists instead of generalists.

MAINTAINER

You are a **MAINTAINER** if your program is primarily focused on sustaining compliance and updating policies to reflect new regulations or is an advanced program that is leveling up niche capabilities. Organizations that were early to the privacy program game and/or organizations that rely heavily on monetizing data are often examples of Maintainers. For the bulletproof, compliance-focused privacy programs with more "rinse & repeat" protocols, hiring tends to focus on plug-and-play people who come from within their industry. Maintainers often begin moving from "accountability" to "being authoritative" in how the business must handle their privacy obligations.

DISRUPTER

If your business is looking for a radical new approach to managing and monetizing data — you may fit the **DISRUPTER** profile. Your privacy program may be poised to be a disrupter of your business to drive bottom line benefits of new approaches to handling data. Organizations that fit the Disrupter profile look for forward-thinking leaders comfortable with being iconoclasts.

"Most organizations have one foot in Builder and one foot in Grower," says Jess Barre, Vice President of Recruitment and Account Management at TRU Staffing Partners. "Now that organizations are seeing privacy as more than a regulatory function, they're beginning to invest in people differently. But that also means they're building the plane while they're flying it."

The Builder, Grower, Maintainer, and Disrupter characteristics apply to privacy programs as well as to the professionals who make them up. Privacy professionals who prefer fast-paced, entrepreneurial environments are more likely to thrive in Builder and Grower programs. Those who are more comfortable with process and routine may be better aligned with Maintainer programs. Disrupter programs are few and far between right now, and they typically look for highly accredited privacy professionals out of Big Tech.

PRIVACY CONTRACTORS ARE NOT A MYTH

With companies across stages of maturity clamoring for privacy resources, contractors offer a great solution in some common circumstances. Contract privacy hiring constitutes 35-55% of available jobs over the past five years. Here are the most common reasons why companies turn to privacy contractors:

LIMITED FULL-TIME EMPLOYEE HEADCOUNT

Hiring managers may have a privacy budget but no approval for full-time headcount. This is common inside Builder and Grower programs. Contract resources can help organizations bridge the gap until full-time roles become available.

PROJECT-BASED WORK

Some types of privacy work, such as contract updates to reflect law revisions, technology implementation, and other project-based work are time-bound. They require a big push then trickle off. The contract privacy talent ecosystem has hit a maturity where organizations can manage these projects with plug-and-play contract resources without committing to long-term base compensations.

SKILL SPECIALIZATION

Many privacy projects require specific expertise — and often, organizations have several of these projects happening simultaneously. It's unusual for one full-time privacy professional to have expertise in all areas, so contractors provide specialized talent for niche skill sets that can be augmented in until they're no longer needed.

RELIEF FOR FULL-TIME EMPLOYEES

One of the fastest-growing problems in data privacy is existing staff burnout. Too much to do, not enough hours. Contract augmentation is the best, if not only, solution to provide relief to your valuable full-time employees with indispensable institutional knowledge.

CHECK THE FIT BEFORE YOU COMMIT

Some privacy programs are not sure who they need, how long they will need them, or who will be the right culture fit — particularly in Builder profiles. Choosing contract-to-hire allows both the employee and employer to experience true day-to-day work life together and determine if further mutual investment is right.

WHAT INTERVIEWS SAY ABOUT OPPORTUNITIES

INTERVIEWS SEND SIGNALS. HERE ARE FOUR WAYS TO SHOW PRIVACY CANDIDATES THAT THEY'RE BEING SET UP FOR SUCCESS.

With privacy jobs, a lot of important decisions get made before hiring managers start talking with candidates. From establishing compensation level and writing a job description to deciding whether a J.D. is necessary for the role, a lot of the work happens up front. But even the most strategically selected candidate pool can slip away to competing offers if the interview process is handled incorrectly.

1. MOVE SWIFTLY

Speed matters, especially for in-demand sectors like privacy. From initial resume submission to the signing of an offer letter, candidates clock how long each step of the interview process takes relative to other companies seeking to hire them.

In 2019, the average time from resume sent to offer extended for a midmarket privacy professional (analyst, specialist, program manager/director) was three to six weeks. Post-pandemic, that timeline truncated to a mere 12 business days in 2021 and the first half of 2022; and 20 business days on average so far in Q3 2022. Virtual interviewing and remote employment have hyper-accelerated the interview process, and companies that have not adapted to this new normal do much more than just lose quality candidates. Slow response times can also leave candidates wondering how important privacy is to an organization.

"If your interview process is weeks longer than the national average, it signals to the job seeker — whether intentional or not — that the organization is not unified in decision making and/or does not place enough importance on this role within the organization," says Jess Barre, VP of Recruitment and Account Management at TRU Staffing Partners. "Privacy pros are hesitant to work for organizations that struggle with decision making or show a lack of buy-in regarding data privacy's value during the interview process."

2. BE EFFICIENT

Another way organizations can show candidates that they value their time and expertise is by reducing the volume of interviews. It's not just about how fast an interview process goes but also how efficiently — meaning, lacking in redundancy.

"When candidates need to talk to seven or more people during the interview process, it signals that this is not a place where things get done efficiently," says Barre.

Especially with net-new privacy positions, there can be a tendency to want to gain consensus from all stakeholders — vertically and laterally. Resist the urge.

"An unnecessarily high number of interviewers signals to privacy candidates that key stakeholders may not be comfortable making data privacy human capital decisions, and more often than not exposes inconsistencies across the enterprise in perspective, buy-in, and understanding of privacy's place within the org to the job seeker," says Barre.

3.

ALIGN ON EXPECTATIONS

With new privacy positions, it's also important to gain organizational alignment on the expectations for the role.

"Privacy candidates sometimes interview with various stakeholders, and everyone has a different opinion on what defines success for the role," says Barre.

A unified understanding across interviewers about not only the responsibilities of a privacy role, but also how success will be measured, sends a strong signal that the individual and the role will be valued by the organization.

4.

EMBRACE IMPERFECTION

Regardless of where an organization is on its privacy journey, it always pays to be honest with candidates. During interviews, provide a look under the hood of where things stand currently and how long-term planning for privacy is shaping up.

"Even if you're at the early stages of institutionalizing privacy into your organization, don't be scared to disclose some of the inner workings of your privacy program (or lack thereof) and show the job seeker the impact opportunity. That means embracing imperfection," says Barre. "It makes privacy candidates feel like they can effect change and stimulate growth, not just maintain the status quo."

TRU CONTRACTORS BY THE NUMBERS

91%: CONTRACT ENGAGEMENTS TRU RECEIVES ARE FILLED SUCCESSFULLY

92%: TRU CONTRACTORS FINISH THEIR ASSIGNMENT, CONVERT TO DIRECT HIRE, OR ARE STILL ON ASSIGNMENT

35-55%: BETWEEN A THIRD AND A HALF OF CURRENT WORKING PRIVACY PROFESSIONALS ARE CONTRACTORS

WANTED: PRIVACY ENGINEERS

Technology and legal are separate worlds within most organizations. However, these two planets are expected to collide with increasing frequency as privacy expertise is needed outside of the general counsel's office.

"Right now, you have privacy lawyers and privacy technicians. Privacy lawyers have been in high demand for many years," says Rachael Haher, Vice President, Business Development and Account Management at TRU Staffing Partners. "A shift is coming. The technical privacy professional is the next big talent pool that we have to create."

Traditionally, privacy impact assessments are performed after most of the engineering work is completed. Now forward-thinking companies are approaching privacy by design, meaning that privacy is considered from the very beginning of a project.

"It's a waste of time, energy, and resources for engineering teams to create products that won't go to market because they're unethical or present too much risk related to privacy law," says Haher. "Privacy needs to be thought about at the onset of development."

While some privacy professionals may take it upon themselves to start learning how to code, the technical-privacy pool is most likely to fill up with trained engineers who develop privacy skills.

"It's going to be easier for engineers and people with technical backgrounds to learn privacy rather than the other way around," says Haher.

For engineers who want to take their careers in the direction of privacy, the IAPP's certification for tech professionals (see next page) is a great way to validate privacy knowledge and signal expertise.

> ***"A shift is coming. The technical privacy professional is the next big talent pool that we have to create."*** — Rachael Haher, CIPM
> VP of Business Development & Account Management

PRIVACY CERTIFICATIONS

TRU doesn't only help clients attract the best privacy talent in the business — we also help the privacy community create new professionals and grow their skills.

TRU Staffing Partners is the only North American staffing partner with the IAPP that is a third-party reseller of their certifications. This year, TRU is proud to offer a direct pipeline for B2C candidates & job seekers to get IAPP online training direct from TRU Staffing Partners.

WANT TO LAUNCH YOUR CAREER WITH IAPP CERTIFICATIONS? SCAN THIS QR CODE TO GET ACCESS TO ONLINE TRAINING BUNDLES THROUGH TRU.

The International Association of Privacy Professionals (IAPP) offers the gold standard in privacy certification programs. While not all privacy jobs require certification, almost all hiring managers desire them. These acronyms show hiring managers that a candidate is serious about privacy. Additionally, we're proud to grant scholarships to deserving privacy professionals every year as part of TRU's annual scholarship program. The program has granted more than $300K in no-cost training and education to deserving professionals since its launch more than a decade ago.

MOST DESIRED PRIVACY CERTIFICATIONS

CIPP – CERTIFIED INFORMATION PRIVACY PROFESSIONAL

Focused on laws and regulations, the CIPP certification is the global standard for becoming an expert on privacy laws, regulations, and frameworks.

CIPT – CERTIFIED INFORMATION PRIVACY TECHNOLOGIST

For engineers and IT professionals, a CIPT certification is the industry benchmark for tech professionals looking to validate their knowledge of privacy requirements.

CIPM – CERTIFIED INFORMATION PRIVACY MANAGER

The CIPM stamp of approval is the first and only privacy certification for professionals who manage day-to-day operations.

PLS – PRIVACY LAW SPECIALIST

The IAPP is accredited by the American Bar Association to certify lawyers in the specialty area of privacy law. US attorneys who meet IAPP's rigorous specialist designation requirements may be permitted under their state's rules of professional responsibility to advertise their specialization in privacy law. PLS-credentialed attorneys must hold two IAPP certifications, pass the PLS Ethics Exam, prove ongoing and substantial involvement in practicing privacy law, provide references, and engage in rigorous continuing education.

AMERICANBARASSOCIATION

ABA Accredited Lawyer Certification Program

FIP – FELLOW OF INFORMATION PRIVACY

The FIP designation signifies that you've taken the next step in the privacy profession. You've demonstrated comprehensive knowledge of privacy laws, privacy program management, and essential data protection practices through successful completion of two IAPP credentials.

IAPP Fellow of Information Privacy

WANT TO APPLY FOR TRU'S SCHOLARSHIP PROGRAM? SCAN THIS QR CODE TO LEARN MORE ABOUT THE APPLICATION PROCESS.

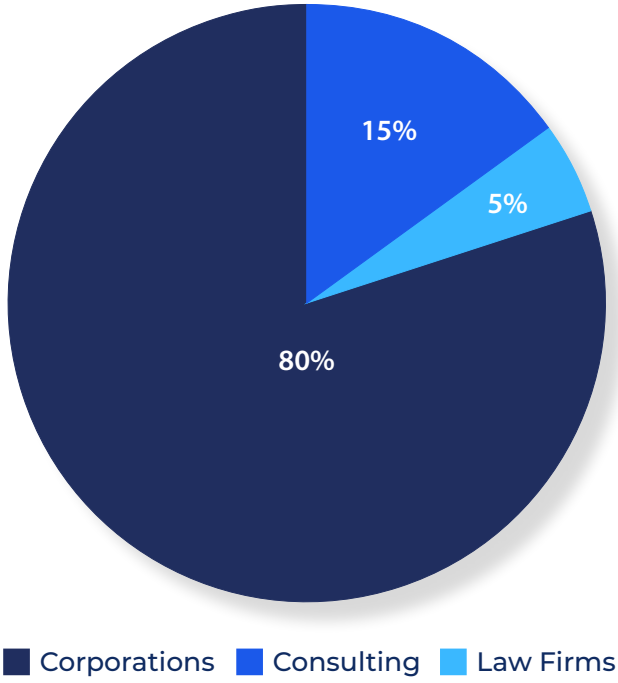
State of the Privacy Job Market 2023

PRIVACY IS HAVING A MOMENT

TRU has been tracking job market trends since 2010 and regularly produces data privacy jobs reports, delivering metrics and analysis hiring managers and job seekers need to stay ahead of the competition.

In a post-pandemic job market, time-to-hire from resume submission to offer acceptance has truncated significantly, and the metrics above are what TRU believes to be the "new normal" speed of hire.

WHERE ARE THE 2022 & Q1 2023 JOBS IN PRIVACY?



TOP 5 MOTIVATIONS OF JOB SEEKERS IN 2021/2022

1. Working remotely/hybrid
2. Mentorship/new leader
3. $$$$$$$
4. Upskilling
5. Diversity, equity, & inclusion

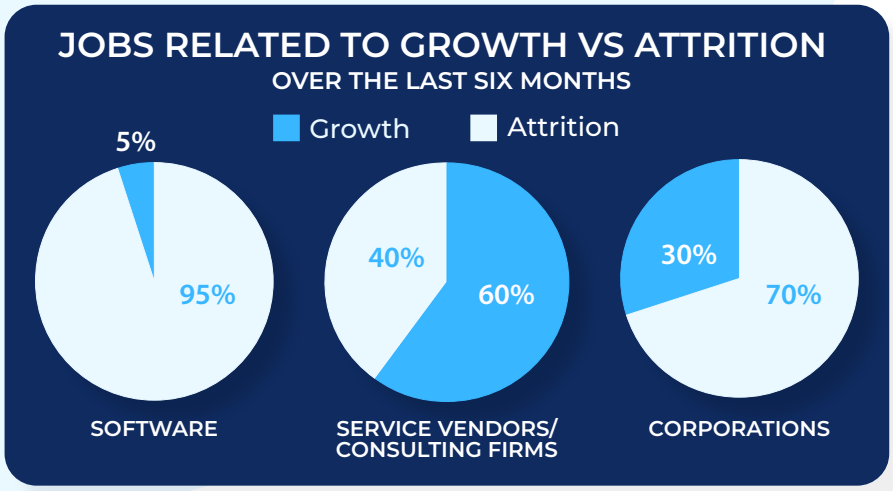
VS.

TOP 5 MOTIVATIONS OF JOB SEEKERS IN 2023

1. Working remotely/hybrid
2. More challenge/opportunity
3. $$$$$$$
4. Commitment to training
5. Company culture/buy-in

TRU TRENDS

- **89%** of new hires are now remote or hybrid
- **3 out of every 5** placements have been contract in Q1 of 2023
- Candidates entertained an average of **2 offers** at the time of acceptance
- **100%** of first-round interviews were virtual in 2021 and 2022
- Law firms with in-office requirements extend hiring timelines an additional **90-120 days**
- **22-40%** base compensation increase for midmarket professionals at point of hire in 2022



COMPENSATION METRICS

Salaries have stayed flat since Q3 2022, but a third of TRU clients go above their range.

Entry Level	**$60K - 85K ($70K - 95K)**
Privacy Analyst/ Specialist	**$90K - 140K ($90K -165K)**
Privacy Program/ Project Manager	**$140K - 180K ($165K - 250K)**
Privacy Sr. Manager/ Consultant	**$140K - 200K ($160K - 250K)**
Privacy Directors/ SMEs	**$200K - 300K ($230K - 400K)**
Privacy Engineer	**$150K - 300K ($175K - 460K)**
Privacy Counsel	**$175K - 325K ($200K - 450K)**
CPOs/ Business Unit Privacy Leads	**$225K - 465K ($275K - 1.5MM)**

BASE SALARY IS FOLLOWED BY TOTAL COMPENSATION IN PARENTHESES.