



# The Hidden Costs of Processing Privacy Requests

Includes **a free, customizable cost calculator template** to help you understand the direct and indirect costs of your company's privacy program.

We believe there are a few fundamental reasons why every company should proactively invest in their privacy request infrastructure.

This means privacy infrastructure technology that orchestrates and fulfills privacy requests (sometimes referred to as data subject requests or DSRs) without any human intervention unless required.

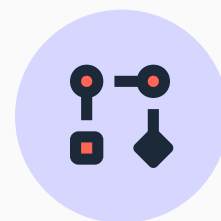
## 01—

Doing so **drives more strategic use of finite internal resources**, repurposing (non-scalable) headcount costs into scalable technical solutions, with remaining resources available to reinvest into privacy innovation.



## 02—

Flexible, well-engineered infrastructure **future-proofs against future regulatory headwinds** and any new data rights (Virginia's new privacy law is a great example of this).



## 03—

It allows **de-risking of one of the most sensitive forms of data a business hold**, through the thoughtful selection of security-conscious solutions that include end-to-end encryption, zero trust integrations, and more.



In forming our model, we spoke to privacy program professionals across company sizes and analyzed financial models they'd prepared to break down the unit economics of an erasure or access request, and the potential ROI of taking a more efficient approach.

As this Calculator shows, manually processing privacy requests or partially solving the problem with some optimization still leaves your organization with a program that is inefficient in the long run and unable to scale with increasing volumes—driven by both customer growth, and continued waves of privacy legislation.

In the following pages, you'll gain an understanding of the hidden costs of your current program, which will help in calculating the ROI of your current privacy program. Most importantly, you'll learn where opportunities exist to invest strategically and drive more efficiency and ROI for the business.

You'll also get a detailed calculation template to tailor to your organization—alongside our simplified web calculator—so you can evaluate the efficiency of your privacy request program.

### **Wait, can I just skip to the free template?**

You can, but we'll hope you read the rest! If you do, you'll leave with:

1. You can, but we'll hope you read the rest! If you do, you'll leave with:1. A line-by-line understanding of the costs that go into maintaining a workflow-reliant manual or semi-automated privacy request program, including variable costs, fixed costs, and more.
2. An “under-the-water-line” understanding of the costs to help you understand the true ROI to weigh against infrastructure and automation investments.
3. A reflection on the components beyond costs that come from investing early in privacy request infrastructure.

## What we'll cover in this guide:

PART 1

### **The Context »**

PART 2

### **Our Approach to Calculating the Costs of Privacy Requests »**

PART 3

### **The Cost Calculator Template and How to Use It »**

PART 4

### **Running the Numbers—Three Scenarios to Explore »**

PART 5

### **Leveraging Your Results »**

PART 6

### **Final Thoughts »**

APPENDIX I

#### **Non-Calculated Risk Factors »**

APPENDIX II

#### **What Does Privacy on Autopilot Look Like? »**



# 01

## The Context



### A quick look at how we got here

The reality of most privacy programs—unless you possess the budget and teams of a Facebook, Apple, or Google—is that it's been gradually built and iterated upon as privacy legislation has quickly evolved, and new data rights requirements needed to be addressed.

When it comes to untangling the mess of data sprawl from both internal and external systems as GDPR, CCPA, and an ever-growing list of laws demanding it, the work often starts with prioritizing the internal systems where personal data is stored and working with engineering teams to implement scripts to query these systems.


But as you well know, data is not just stored in one place, and the average mid-size company can be leveraging hundreds of SaaS (software-as-a-service) systems, each being a place where personal data can be stored, and by law, must be returned or deleted when a consumer requests it.

When it comes to acting on personal data for access, deletion, or consent requests across both internal and external vendors, most companies will take one of **three approaches to solving the challenge**:

## 01— Manual workflow

Reliant on humans at each stage of the process, from email-blasting vendors to manually querying internal systems and packaging and returning user data.


### WHAT THIS LOOKS LIKE:

- 
- Privacy@ email address for users to email requests
  - Manual inbox reviews, sorting through the veracity of each request, and location-based triaging
  - Manual data scrapes and checks through some systems (oftentimes not complete in all data systems due to manual effort required)

## 02— Semi-automated

May leverage request intake or workflow management software and scripts or code that query a subset of personal data stores but still rely on human actions to collate a user's data.


### WHAT THIS LOOKS LIKE:

- 
- A web form to ingest user requests
  - Workflow management software that helps automate shoulder-taps when action is required (e.g., "Engineering, you have a new deletion request to action!") and that tracks follow-up / completion
  - Some use of automated scripts, APIs, or webhooks to connect priority sources of personal data into the workflow.

### 03— Fully automated

Privacy request systems that can action a request start-to-finish without any human intervention unless mandated through zero-trust API-based integrations and other system hookups.

**WHAT THIS LOOKS LIKE:**

- 
- A self-serve Privacy Center where users can select the appropriate data action (erasure, access, or opt-out, for example), view progress, and view the data in context from an accessible dashboard.
  - Authentication integrated with an organization's existing user authentication methods, like a user account.
  - A completeness of data orchestration through no- or low-code integrations across all external and internal systems.



Our calculator focuses on the costs of manual and semi-automated structures to make the case of why an investment in automation is ultimately a more cost-efficient solution.

Whether your organization receives 1, 100, or 1,000 requests per month, there are three major weaknesses in manual or semi-automated systems:

- › Bottlenecks and delays in scaling with unexpected spikes
- › Unavoidable human-error failure points in your organization's system
- › Hidden costs associated with having humans involved in the fulfillment process



#### PROBLEM 1

### **Bottlenecks and delays**

Think of the last time a CEO misspoke or a negative corporate action or privacy policy change was uncovered that landed on the front page of a major publication. The unfortunate reality for the privacy office is that with greater data rights, customer revolt will only continue to lead to swift backlash in the form of deletion requests. These manual and semi-automated approaches are not built to respond to the rapid-fire inflow of frustrated users requesting their account and data be removed, causing bottlenecks and risking compliance delays.



#### PROBLEM 2

### **Unavoidable human error**

We explore this a little later in this guide, but suffice to say that when humans are involved in the handling of personal data gathering—even with a robust training program—you need to be accounting for risks such as incomplete collection of data from certain systems, or worse, the wrong data being erased or returned.



#### PROBLEM 3

### **Hidden costs**

**This is at the heart of what our Privacy Request Cost Calculator solves.** It helps you unpack the aggregate costs of your privacy request program, including how to think about your organization's costs, efficiencies, and potential ROI.





# 02 Our Approach to Calculating the Costs of Privacy Requests

In developing our calculator and spreadsheet template, our focus was on quantifying the time costs of each stakeholder involved in the process and the fixed costs incurred—regardless of how many requests your organization receives.

But in putting together our analysis, we didn't just want to break down and then write up what we found—we wanted to build a tool to enable you to run your own calculations, so we created a **free, customizable template where you can input your own numbers and edit as required.**

Start by [downloading the template](#) and making a copy (go to File > Make a copy). Then, let's get to work on discovering the costs involved in your privacy program.

[Access the template.](#)

## What's involved in each request?

Before diving in, let's take a high-level look at what makes up the costs and processes in a standard privacy program.

We found that **the cost of a privacy request can essentially be broken down into three categories**. In our calculator, this is how we've bucketed the line items involved in a typical non-automated privacy request workflow.



### CATEGORY 1

#### Variable, or “per request” costs

**Direct costs** that are incurred with each request and are **variable based on volume**. Think of these as the time each stakeholder is engaged at every step of the process to ensure a request is handled from submission to return.



### CATEGORY 2

#### Fixed program upkeep and maintenance costs

**Fixed costs** that generally don't increase or decrease once a company is required to comply with data access legislation. This includes things like integrating new data stores into existing queries, adding new external systems, auditing tickets for quality control, and other miscellaneous items. We've also tried to factor an allowance for reactive intervention into your program if a PR storm or slipup requires executive-level involvement.

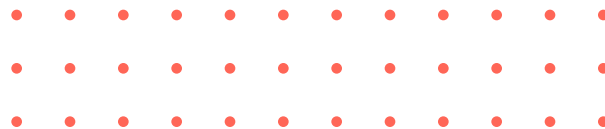


### CATEGORY 3

#### Non-calculated program risks

Costs that are tricky to calculate on a per-request basis (and aren't included in our calculators) but nonetheless are ever-present risks in a privacy request workflow that is reliant on human involvement, including penalties for non-compliance and more.

You can see what we've included in each of these categories by [accessing the calculator template](#) and going line-by-line. We also explore Category 3 in more detail in [Appendix 1](#).



# 03 Understanding the Cost Calculator Template

If the spreadsheet template seems overwhelming at first, know that there are essentially four main sections:

## 01— Key Calculator Inputs

Start here by inputting the basics of your privacy program, including the number of privacy requests you receive in an average month and the number of external SaaS systems your company stores user data in (think of platforms like Marketo).

**A note on internal systems:** Internal systems are not a variable input because these are often batch queried together. However, this is included in the overall calculator under Category 2.

*Note: If you have a more manual process for retrieving data from internal systems than average in the calculator, you can edit cell D18 and add a “time per request” estimate for how long this process takes your organization.*

## 02— Privacy Request Calculations

This is where the number-crunching begins! In this section, you'll see how we've broken out the three categories identified on page 10 and under each, what we believe are the most common components of each one.

In Column C, you'll see a brief description of each line, and column I covers any assumptions included in the calculations.

Some cells are shaded to help you understand the areas where you can tweak to fit any program specifics of your company. You can always add new lines, too—just make sure that any relevant formulas are copied down or unaffected.

**Remember:** values in **Category A largely vary with the number of requests, whereas Categories B and C are largely fixed and unaffected by the number of privacy requests a company receives** (we've noted otherwise where that's not the case).

*Note on Category C – Non-calculated program risks: See [Appendix 1](#) for more details on what we see as tricky to calculate yet still crucial to factor into any manual or semi-automated privacy program.*

## 03— Hourly Rates

The third tab of the Cost Calculator spreadsheet is a table of stakeholders and salaries—based on general estimations of the stakeholders that might be involved at various stages, from request intake to data gathering and other inputs.

Hourly rates are broken out to ensure an accurate calculation of cost based on the steps each person is involved in.

**Tip:** You can either leave these unadjusted or edit these to reflect local conditions and your organization's costs.

## **04— Results**

The most important part—here's where you can see the hard costs of your organization's privacy program and approach. These costs are broken out in a few different ways—including the total monthly and annual costs, an estimated cost per request, and the aggregate time spent processing per month—so you can use whichever is most appropriate for your internal analysis and to help make a business case for more strategic privacy investments.

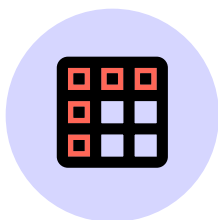
Now, you're across the components, let's move to trying out a few different scenarios.



# 04 Running the Numbers— Three Scenarios to Explore

In this section, we'll look at a few different scenarios you can run to ensure there are no blind spots in your organization's current program and approach.

Watch the **Results** section closely—this is where you'll see how each can impact the program budget and team's time.



## SCENARIO 1

### Baseline

This should be the first set of numbers you input based on current average monthly privacy request volume, the number of external or SaaS data processors your organization leverages, and salaries.

Regardless if you go further, these baseline numbers can be incredibly useful in helping to benchmark the real program costs, and if not aligned to business expectations, advocate for more strategic infrastructure or engineering investments.



#### SCENARIO 2

### Two Years Ahead

Take your organization's baseline numbers and multiply these by any data you have on year-over-year customer or user growth to try and predict what privacy request volume could look like two years from now. Don't forget to also increase the number of external systems you expect to be leveraging for personal data processing, too.

You can also model further out using this scenario to build accurate forecasts for strategic long-term privacy program investment.

*A legal lookahead: Don't underestimate the impact of impending consumer-centric data privacy laws at a state, federal, and global level in your forecasting. It's highly likely that, particularly if a U.S. federal privacy bill is passed with CCPA-esque privacy rights, a majority of your organization's user base could be covered by such laws and possess greater awareness of their rights to reclaim their data.*



#### SCENARIO 3

### The Unexpected Spike

We've mentioned this earlier, but it's useful to be prepared by understanding how a bad PR moment, corporate misstep, or unwelcome Privacy Policy can quickly turn into a user deletion backlash as seen over and over again.

For this scenario, we suggest you **multiply monthly average privacy requests times ten** to understand the impact such an event would have on your organization's ability to stay in compliance with data rights requests and legally mandated time frames.





# 05 Leveraging Your Results

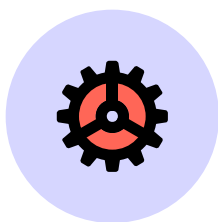
In sum, the goal of using the Privacy Request Cost Calculator is simple: empower you and your team to make smarter decisions about the future of your organization's privacy program.

Once you've taken the time to explore the scenarios or use the spreadsheet calculator to tinker with each line item if you choose, there are a number of tangible situations in which you can leverage your findings:



## **Your next quarterly business review**

Leverage the results of the Privacy Request Cost Calculators and the forward predictions from Scenario Two to anchor your strategic initiatives and investments in tangible modeling.



## **Process optimization assessments**

Using the spreadsheet template, you can see which parts of your manual or semi-automated process may be incurring the biggest time sucks and focus on quick-win improvements. Is one particular data processor taking an above-average time to respond to deletion requests? Is a particular internal stakeholder slowing the process down or increasing risk through unnecessary back-and-forth containing personal data?



## **Vendor assessment conversations**

Leverage the calculator as a cost-benefit analysis tool for assessing privacy vendors. Look for how much of the manual workflow or internally-built pieces of automation can be eliminated, and compare this against licensing or platform costs.

# 06

## Final Thoughts

Our end goal in studying the economics of processing privacy requests was never to solely quantify the dollar costs of the process.

Instead, this calculator proves the **value of strategically investing in your organization's privacy program and the tools to optimize proactively**, rather than in response to a privacy snafu or when teams are at their breaking point.

As you'll see in [Appendix Two](#), moving to a posture of proactive optimization and investing early in your data privacy infrastructure can bring multiple benefits.

**Even ignoring the benefits you can derive for security and user experience for a moment**—investing early in an optimal privacy architecture can quickly deliver savings to the business tomorrow and an insurance policy for any storms ahead. (See Scenario 3 in our [Running the Numbers](#) section for what an investment here can prevent.)

We hope you find the Privacy Request Cost Calculator useful in proving your program's value. We'd love to hear your thoughts as you try the calculator, too—you can email us with feedback at [privacycalculator@transcend.io](mailto:privacycalculator@transcend.io).

## APPENDIX I

# Non-Calculated Risk Factors

In building a generalized model, we realized that outside the variable and fixed costs of processing privacy requests, there was a third bucket that was more complicated to average across each request yet still was crucial when assessing the ROI of manual or semi-automated programs.

1. **Risk of penalties:** These are the most objective risks in Category C—think of these as the fines per reported data rights violations under GDPR or CCPA and any incoming future state-based or country-based regulation.
2. **Risk of data breach.** If your organization is manually requesting deletion from a vendor over email, one slipup in an email address could be enough to cause a data leak from your system. Worse, if a non-trustless vendor requires your system keys to be stored, a breach of their system could expose your entire data store. According to IBM's Cost of a Data Breach Report 2020, a data breach can cost an organization an average of \$3.86 million U.S. per incident.
3. **Risk of human error.** If humans are involved in your privacy request workflow, you can't ignore the risk of human error entering the equation. At best, this might be a typo or forgotten attachment, but at worst, we've received stories of companies returning the wrong person's data, which can lead to penalties and data breach risks.
4. **Risk of brand damage.** In the above scenarios, what if one of those slipups in your program impacted a celebrity, politician, or influencer? Or if a data breach impacts a large swath of your user base? The brand damage based on consumer backlash, translating to product usage and revenue—from just one slipup—can get real, fast.

## APPENDIX II

# What Does Privacy on Autopilot Look Like?

We've spent the majority of this guide centered on the costs of manual or semi-automated privacy request programs and infrastructures.

What are the benefits that investing in privacy infrastructure and end-to-end automated technical solutions like Transcend can present?

If you take those minutes, hours, and dollars spent on manual triage and process, what opportunities does that present for **privacy innovation and leadership beyond compliance? Further, what value-adds does that deliver to the business?**

An important detail to watch out for: Not all solutions that claim “automation” are factual. As we mentioned earlier, when assessing privacy request solutions, make sure that you're reviewing software that removes work from your team's plate rather than adding to it. *(In this case, being made redundant from the process is a good outcome!)*

Also, remember the **Five S's of Best-In-Class Privacy**:

### 01 — Scalability

One of the biggest risk areas for workflow-based privacy request structures that are reliant on humans is the inability to respond to high volumes of privacy requests or to grow in a resource-efficient way as the business continues to grow. That risk is eliminated in code-based systems that can easily scale without sacrificing requests.

## APPENDIX II // WHAT DOES PRIVACY ON AUTOPILOT LOOK LIKE?

### 02 — Security

Moving to privacy infrastructure over manual workflow means that a number of additional measures can be leveraged to further enhance your organization's security posture. This includes replacing email trails with end-to-end encryption when data is transferred between your data stores and your users and an ability to leverage more robust user authentication methods.

### 03 — Superior user experience

Without human dependencies, privacy requests can be securely ingested, verified, compiled from across internal data stores and SaaS systems, and returned in a user-friendly manner in a fraction of the time—and well within mandated time frames.

## The Privacy Halo Effect

Two statistics to consider when evaluating the importance of user experience on privacy and how it can be a powerful brand-building opportunity:

**60%** of Americans say companies that can provide users with instant access to control personal data are seen to care about their customers.

Additionally, **62%** of Americans also rate companies that provide instant access to a user's data as trustworthy, **58%** say transparent, and **55%** deem them to be helpful.

SOURCE: TRANSCEND'S [DATA PRIVACY FEEDBACK LOOP SURVEY OF 1,000 AMERICANS](#), CONDUCTED IN 2020.

## **APPENDIX II // WHAT DOES PRIVACY ON AUTOPILOT LOOK LIKE?**

### **04 —‘Slipup’ elimination**


Removing humans as much as possible, if not entirely, from your privacy request process eliminates those innocent yet critical slipups when handling sensitive personal data, from exposing sensitive information without adequate verification to returning data to the wrong user. Privacy request automation leverages deterministic queries to ensure that only the right consenting user’s data is being operated on.

### **05 —Strategic focus**

Finally, and as we mentioned in our Findings, migrating to an automated model frees your team from the operational weeds and allows them to focus on strategic work to improve your organization’s overall privacy experience for customers and users or get back to operating on revenue-generating code or operations.

It also frees up your legal team from having to act as pseudo product managers in trying to patch internal solves with your engineers and allows them to instead easily add new data stores or systems as required, without code.





## The Privacy Request Cost Calculator is brought to you by Transcend.

At Transcend, we're big believers in investing in engineered solutions to privacy's greatest challenges with a security-centric and future-proof architecture for scalability and user-centric data privacy compliance.

We provide a full-stack solution to receive, manage, and automatically fulfill privacy requests from your users—trusted by leading brands including Patreon, Indiegogo, Robinhood, and more.

Free up engineering resources, meet—exceed—regulatory obligations with auditable automation, and build brand trust through respectful data and consent transparency and control.



**Speak to our solutions team »**



**Learn more at [transcend.io](https://transcend.io) »**



