## The Age of Privacy:

# The Cost of Continuous Compliance

### Benchmarking the Ongoing Operational Impact of GDPR & CCPA

Updated February 2020

DATAGRAIL®

datagrail.io

# Summary

## The European General Data Protection Regulation (GDPR) came into effect on May 25, 2018, and even with two years notice only half of companies self-reported as compliant.

**For most companies, it took at least half a year to achieve GDPR compliance. With the benefit of a year in hindsight now, the one thing privacy professionals most wish they would have done differently is started planning and implementation sooner.**

Privacy professionals shared that GDPR compliance was complex to understand and hard to manage, consuming thousands of hours of productivity and introducing risk from error-prone manual tasks. Even worse, they agree that the work they have done to prepare for GDPR compliance does not scale to support new privacy regulations.

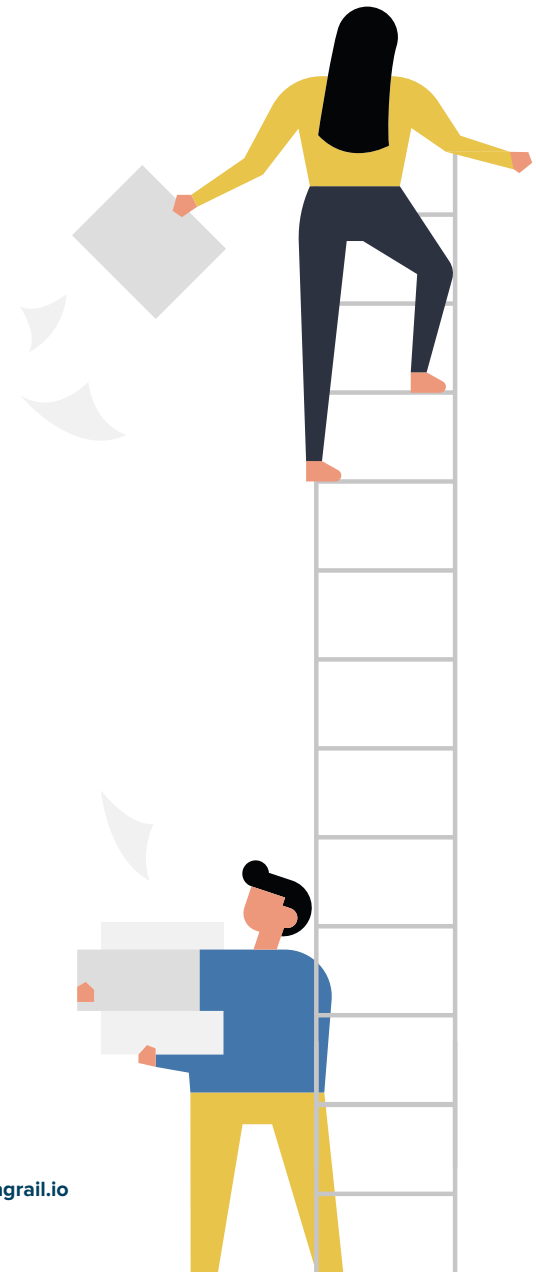
The cost of privacy compliance is more than financial - it is operational and it is an ongoing cost. In the approach to GDPR, companies assigned scores of employees to dozens of meetings, consuming hundreds of hours of work to get their company ready. When you do the math it's a doozy: some companies spent more than 9,000 hours in meetings in the lead up to GDPR. Even senior decision makers spent weeks of their time, not only to prepare for GDPR, but also to sustain compliance. Unfortunately, preparation is just an initial checkbox.

Sustaining compliance requires companies to devote employees to thousands of additional hours working on error-prone manual processes. Privacy professionals are challenged to effectively manage workflows across multiple systems and services, and struggle to integrate solutions across multiple systems and services. In an effort to minimize risk, most privacy professionals recognize the importance of reducing human errors related to privacy requests, yet most companies rely on dozens of people to complete an access or deletion Data Subject Request (DSR).

Now, with the California Consumer Privacy Act (CCPA) in effect as of January 2020 and a worldwide wave of impending privacy regulations, some privacy professionals are moving beyond manual workflows and looking for ways to operationalize privacy management to sustain compliance for the long-term. A majority of companies embraced technology solutions, but a much smaller portion have realized the benefits of automation, with only some privacy professionals reporting they automate data inventory. Almost half are still heavily relying on cumbersome questionnaires or surveys and email-based workflows.

Compliance has a massive operational footprint across an entire organization, but technology can help minimize it. Early adopters are using technology to integrate business systems, reduce human error, and support new regulations. Companies that are able to automate the manual processes tied to privacy compliance like data mapping and processing DSRs maximize their efficiency and efficacy to minimize their risk and the cost of continuous compliance.

# Highlights



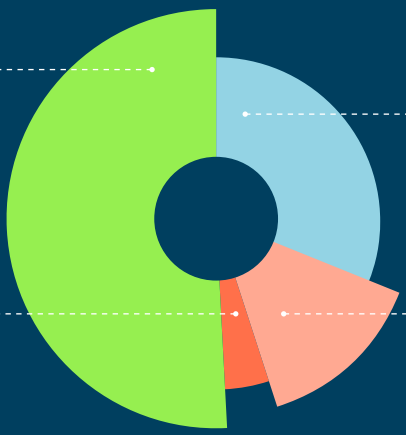
- **70%** of respondents agree that the systems they put in place (or will be putting in place) will **not** scale as new regulations emerge.
- **9 out of 10 companies** plan to hire at least **3 people** to manage privacy regulations in the next two years.
- **9 out of 10** privacy professionals agree a data inventory is critical to becoming compliant with existing and forthcoming privacy regulations.
- Only **51% of companies achieved self-reported GDPR compliance** by the May 25, 2018 deadline; most took more than six months to prepare.
- It's likely the average **organization spent 2,000 - 4,000 hours in meetings alone preparing for GDPR** - that's more than a full year of work.
  - 49% of decision makers personally spent 80 hours preparing for GDPR.
  - 34% of decision makers at enterprise companies (1000+ employees) spent at least 160 hours personally preparing for GDPR.
- 67% of companies had at least **25 employees** involved in managing GDPR readiness; **44% of companies had at least 50.**
- 58% of companies are receiving **11+ Data Subject Requests (DSRs)** per month, **28% are getting 100+ DSRs** per month.
- 58% of companies have at least **26 employees managing DSRs**.
- Companies are concerned about human error when it comes to processing privacy requests, as **84%** of them have a process to prevent manual DSR errors.
- **Technology adoption rates are lower for CCPA than GDPR;** companies are primarily relying on employee training (61%) and new policy and process creation (53%) to comply with CCPA.

# GDPR, One Year Later

By the end of 2018, most US companies (82%) self-reported achieving GDPR compliance, while the remainder plan to become compliant by the end of 2019.

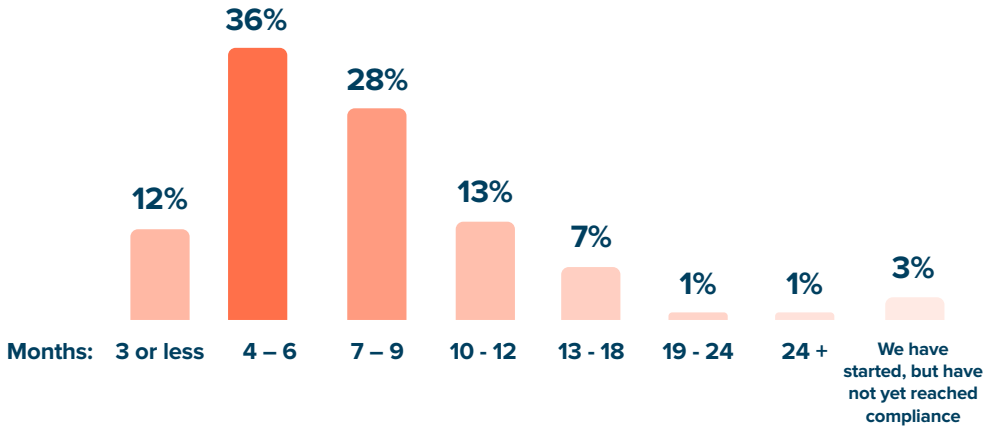
The bad news is that it took longer to achieve compliance than expected - most companies (53%) spent more than six months getting ready.

## Self-reported Achieving GDPR Compliance




***Only 51% of companies achieved self-reported GDPR compliance by the May 25, 2018 deadline.***

### Time Spent to Achieve GDPR Compliance




Privacy professionals took a multi-pronged approach to GDPR compliance, with various levels of sophistication. A majority have embraced technology solutions, but half are still using manual processes to identify the location of personal data and to manage Data Subject Requests (DSRs). Not only do these manual processes introduce risk because they are error-prone, but they can also be very time-consuming.

# Approaches taken to become GDPR COMPLIANT

**58%** Purchased commercial technology solutions

**57%** Developed internal technology solutions

**43%** focused existing employees to oversee privacy management

**48%** Developed manual processes to manage data subject requests (the right to be forgotten, portability, etc.)

**50%** Hired external consultants/legal counsel

**46%** Hired employees to focus on privacy management

**54%** Established appropriate stakeholders and an internal workflow and manual processes to identify the location of regulated data

*"The biggest pain points are data breach disclosure requirements and the removal of data from many locations."*

# The Continuous Cost of Compliance

**The cost of compliance cannot be measured in dollars alone: it must also include the operational expenses of human resources and time.**

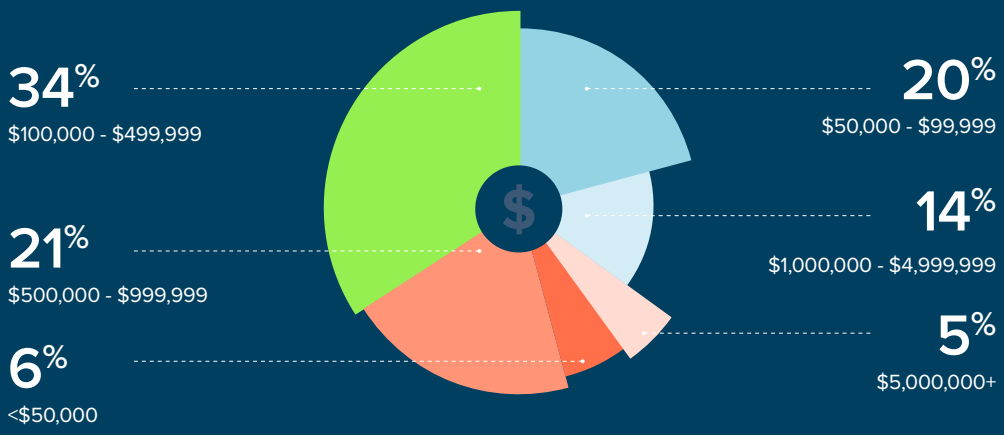
Likewise, these measurements must extend beyond the initial cost of preparation to examine sustained compliance. Companies spent hundreds of thousands - even millions - of dollars on compliance solutions, but they continue spending thousands of hours manually managing compliance at the risk of introducing human error.

### The Cost of GDPR Preparation

Benchmarking the financial cost of compliance as a baseline, 74% of companies spent more than $100,000 on compliance consulting services and technology solutions, and 20% spent more than $1M.

One-third (34%) of enterprise companies (1,000+ employees) spent more than $1M.

**Company Spend on Consulting Services and/or Technology**



**There were multiple human factors working toward GDPR compliance, each with a multiplicative effect on its true cost.**

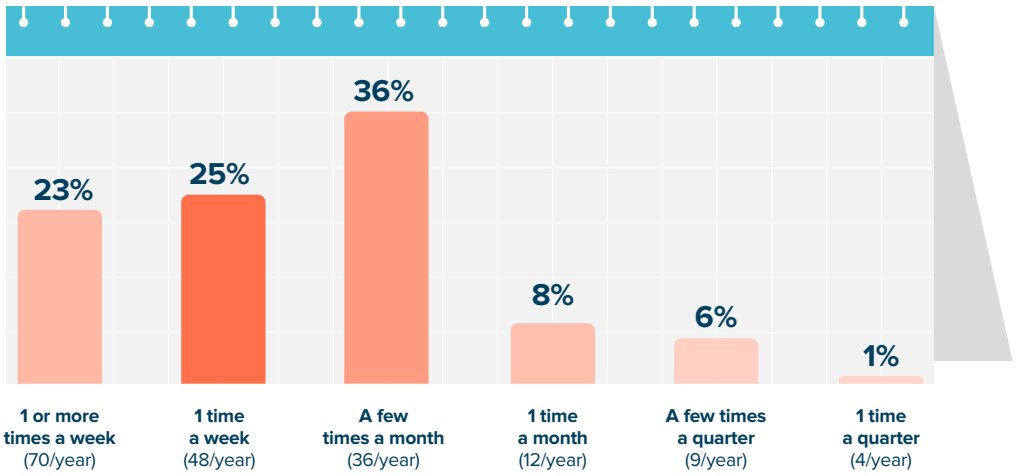
Most organizations (84%) met a few times a week preparing for GDPR, and 67% of companies involved 25+ employees in the preparation process. The end result was a large number of employees involved in an increasing number of meetings at a large opportunity cost.

The effect was even worse for enterprise companies, who had twice as many employees involved in preparing for GDPR as compared to those with less than 1,000 employees.

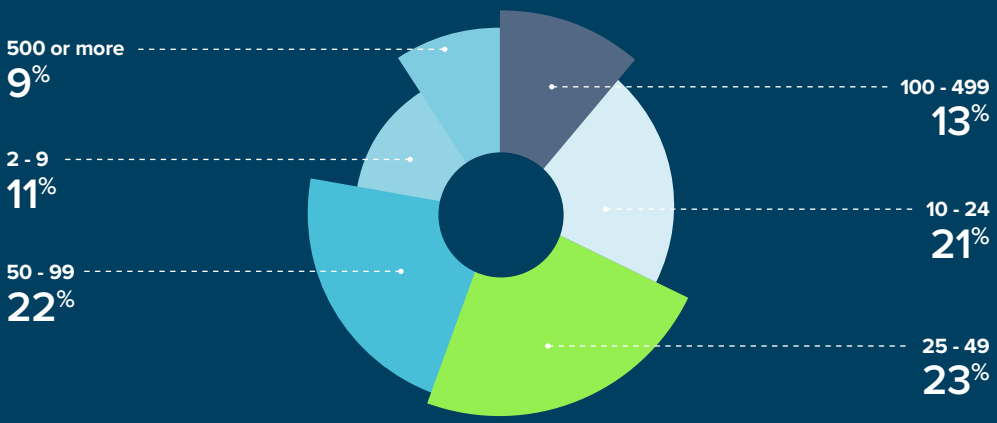
One-third of enterprise decision makers personally spent more than 160 hours preparing for GDPR.

***Two-thirds of organizations had 25 or more employees involved in managing GDPR, and 80% of organizations met at least a few times a month.***

**Meetings Held in Year Leading up to GDPR**




**Employees involved in managing GDPR compliance initiatives and process**

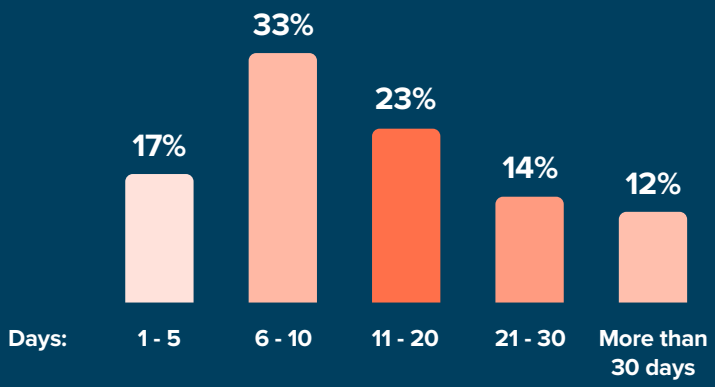



We conservatively estimate that the average company spent 2,100 hours in meetings alone. Enterprise companies could have spent over 9,000 hours in meetings, and thousands of additional hours preparing for GDPR. Senior decision makers specifically spent weeks of their time to prepare for GDPR.

Ultimately, the impact of all this is reflected in the opportunity cost of diverting dozens of employees (and specifically decision makers) to unpack GDPR, as well as the risk of human error from so many employees managing the process.

## Time spent by decision makers *preparing* for GDPR

(1 day = 8 hours)

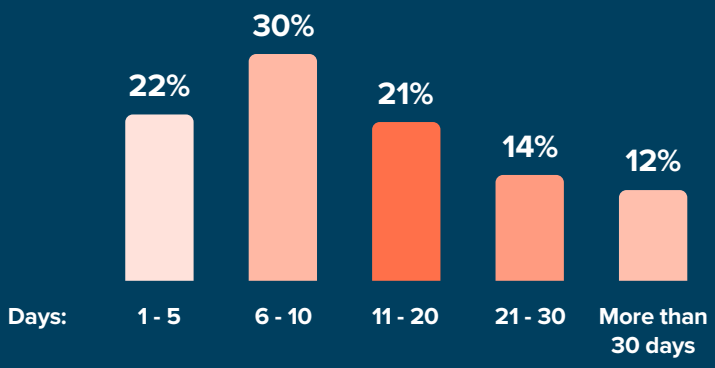



### The Cost of *Sustained* Compliance

Preparing for GDPR likely involved a set of activities such as data inventory and mapping, establishing a workflow (whether automated or manual) for processing DSRs, implementing consent management, and updating privacy policies. Sustaining that compliance, however, involves further activities such as continually updating the data map with new fields and business systems, communicating process changes with all employees involved, producing robust compliance logs, and staying current with regulation updates or changes - in addition to processing DSRs that come through. Decision makers report spending virtually the same amount of time working to sustain compliance as they did to prepare: **this is the cost of continuous compliance.**

## Time spent by decision makers *sustaining* GDPR

(1 day = 8 hours)

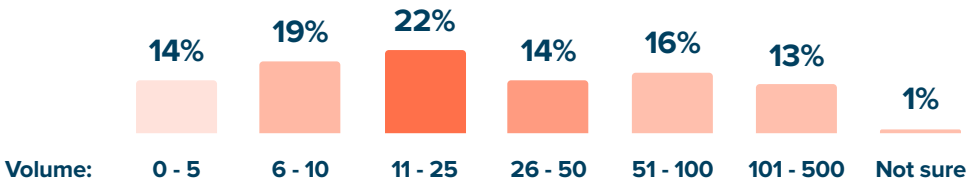




More than half of companies implemented manual processes to identify the location of regulated data, and almost half developed manual processes to manage DSRs.

Considering that two-thirds of companies are managing a double-digit number of systems subject to DSRs, those manual workflows add up to a lot of lost time and introduce a lot more risk of human error.

**Number of systems services subject to DSRs**

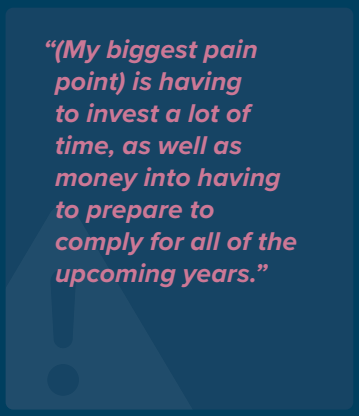




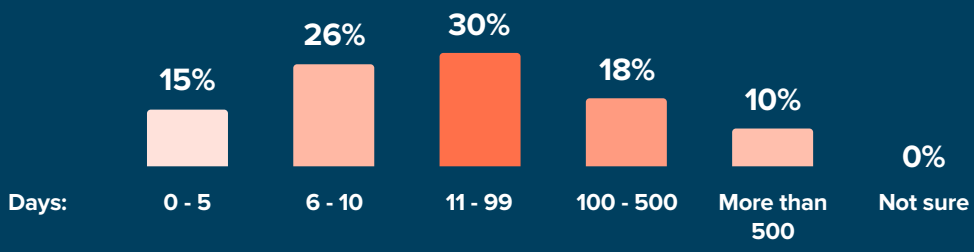
Even though 84% of privacy professionals self-reported that they had a process to prevent human error in their DSRs - a clear sign they were aware of the risk - most companies are still manually processing them. Additionally, companies are receiving a high volume of requests:

- More than half (58%) of companies are receiving 11+ DSRs per month. 28% are receiving 100+ per month.
- More than half of companies (58%) have at least 26 employees managing these requests.

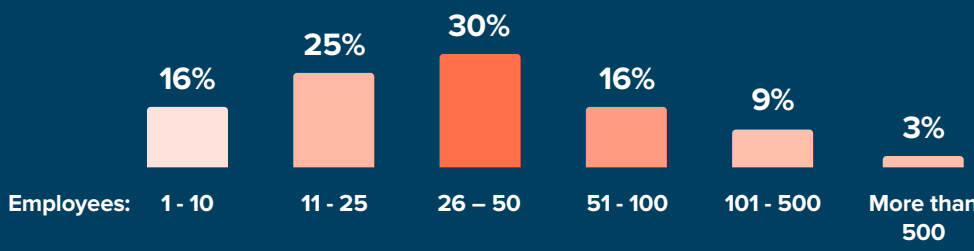
Conservatively extrapolating, thousands of emails or alerts have been sent to manage DSRs in the past year, increasing the magnitude of risk with each touch point. DSRs are a key requirement of GDPR, yet without an automated solution each additional human resource assigned to its management decreases efficiency and increases risk. **Companies will continue to pay the cost of compliance and bear associated risks unless they are able to operationalize manual tasks, workflows, and processes associated with ongoing compliance.**




**Volume of Data Subject Requests (DSRs) per month**




**Number of employees involved with processing a single DSR**



# A Year Later, Lessons Learned

**Complying with new regulations is never easy, and time is rarely on your side. Most frequently, privacy professionals were challenged by the complexity of GDPR and the lack of a clear path to compliance.**

From an operational standpoint, privacy professionals found it difficult to manage workflows across multiple systems and services and struggled to integrate solutions across multiple systems and services. Unfortunately, 70% of respondents agree that despite their invested time and effort, the systems put in place will not scale to support new requirements as additional regulations emerge. In other words, the processes and solutions implemented by these organizations will likely struggle to support the complexity of new and changing regulations due to different requirements across data systems involved.

***70% of respondents agree that the systems they put in place (or will be putting in place) will not scale as new regulations emerge.***

**Top five challenges for GDPR Compliance:**

- The General Data Protection Regulations are complex/ vague (56%)
- Regulations lack a clear path to achieve compliance (45%)
- Could not effectively manage workflows across multiple systems, and struggled to integrate solutions across multiple services (39%)
- Not enough time to plan and execute compliance program (32%)
- Not enough human resources to manage and execute program (31%)

**Most frequently, privacy professionals reported that if they could have done one thing differently, they would have:**

1. **Started planning and implementation sooner**
2. **Built a data inventory**
3. **Bought a commercial solution rather than built their own**
4. **Sought out a technology solution**
5. **Hired more people internally**

Companies that didn't have enough time to prepare would have prioritized technology, while smaller teams would have prioritized hiring more consultants to help prepare.

Larger and more prepared companies tended to prioritize the importance of data inventories by a significant margin. Additionally, 90% of privacy professionals agree a data inventory is critical to becoming compliant with existing and forthcoming privacy regulations.

# Complying with CCPA

*"(A big pain point for us is) having our corporate lawyers go over the CCPA and GDPR to understand its complex language so that we can apply it properly to our databases. Also the right to delete is challenging for all of our departments especially our marketing team."*

**Six months prior to the CCPA deadline, most companies (93%) had already started preparing and two-thirds expected it would take less than six months to become compliant.**

However, lessons from GDPR implementations suggest that is optimistic, considering most privacy professionals wished they had more time to prepare.

**The top five challenges for CCPA are virtually identical to GDPR:**

1. The California Consumer Protection Act is complex/vague (50%)
2. Could not effectively manage workflows across multiple systems and services, or struggled to integrate solutions across multiple systems and services (49%)
3. The California Consumer Protection Act lacks a clear path to achieve compliance (43%)
4. Not enough human resources required to execute and manage our compliance program (37%)
5. Not enough internal human resources to develop internal technology solutions (34%)

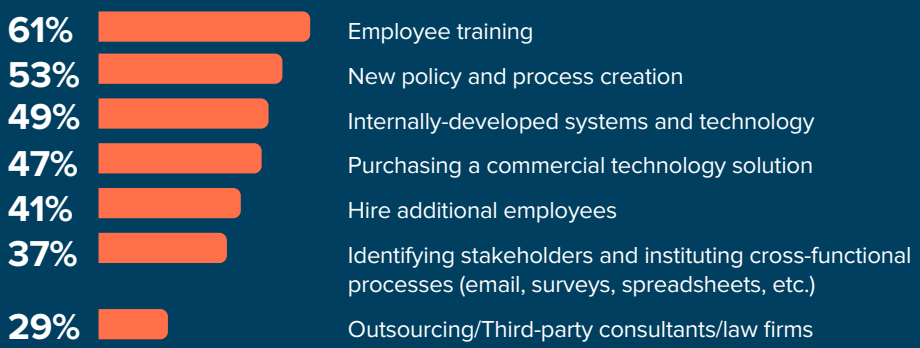
**Most Challenging Elements of the Consumer Rights Portion of CCPA:**

| | | |
|---|---|---|
| 1 | Right of access | **50%** |
| 2 | Right of data portability | **49%** |
| 3 | Right to incentive notice | **39%** |
| 4 | Right to notice | **35%** |
| 5 | Right to opt-out | **34%** |

**Ranking CCPA-specific challenges:**

| | | |
|---|---|---|
| 1 | Implementing processes to de-identify/anonymize data | **42%** |
| 2 | Training employees | **42%** |
| 3 | Updating privacy policies | **39%** |
| 4 | Establishing a records system to monitor data flows | **39%** |
| 5 | Implementing protocols for consumer rights | **37%** |

**Tactics Companies are Taking to Comply with CCPA**




Compared to GDPR preparation tactics, companies preparing for CCPA are focusing on employee training and new policy creation (manual processes to prepare for compliance) more so than implementing technologies (longer term solutions to sustain compliance). By focusing on human resources instead of technology, companies may be challenged to sustain compliance over the long run and to continually support new emerging regulations, despite a large upfront investment in time and effort.

# Looking Ahead - From GDPR to CCPA and Beyond

*"My biggest pain points are ensuring that we have and implement the latest and optimal technology and hire the best employees to be in compliance with the privacy regulations."*

**The Age of Privacy is here.**

**GDPR served as a template for CCPA and a catalyst for socio-economic change.**

An overwhelming majority (79%) of companies are spending at least $100,000 on GDPR & CCPA compliance. Yet, it appears that companies are approaching each regulation on a case-by-case basis, instead of building a solution to support existing and forthcoming regulations: 70% of respondents agreed that the systems they put in place will not scale as new regulations emerge.

Companies are trying to solve data privacy compliance with money and manpower, relying on dozens of employees to manage compliance related issues.

Recognizing that privacy regulations aren't going away, 90% of privacy professionals plan to hire three employees within the next two years to handle forthcoming regulations.

The true cost of the Age of Privacy thus cannot be calculated by the price of compliance solutions and services alone. It includes the cost and risks associated with assigning dozens or hundreds of employees to thousands of hours of manual compliance management, and the opportunity cost when those employees are senior decision makers. **Unless companies take a different approach to operationalize the management of privacy regulations, there will be an ever increasing and compounding cost of continuous compliance.**

The key is to invest in solutions that can automate manual processes and integrate across business systems and third-party services. We can learn from early adopters here-one third (32%) of companies are automatically updating their data inventory, and more than half (58%) have purchased commercial technology solutions.

## To achieve and sustain compliance a company needs to:

1. Understand the complexities and unique requirements of each particular regulation
2. Continually identify systems, both existing and new, that hold regulated data
3. Put practices in place to update those systems when new information is added
4. Operationalize data privacy requests while minimizing processing risks
5. Easily adapt to regulatory changes or amendments that impact any of the above

**Above all, seek solutions that will support new privacy regulations as they emerge and the associated complexities dealing with multiple regulations.**

Integration at the business system level and automation are operational advantages which can minimize the risk and cost of continuous compliance from GDPR to CCPA and beyond.

## Methodology

DataGrail partnered with Marketcube, a third-party research company, to survey 301 professionals involved with the decision-making process as it relates to privacy regulations.

All respondents work at companies with 50+ employees and are affected by GDPR, CCPA, or both. Respondents were surveyed in April 2019.

## About DataGrail

DataGrail helps companies comply effortlessly with existing and emerging privacy laws, such as GDPR and CCPA. With more than enterprise pre-built connectors currently in place, the DataGrail platform provides a 360-degree, real-time view of the applications used and maps the personal data associated with each of those systems.

DataGrail also allows customers to manage their privacy request workflows and email preferences across applications. To learn more about DataGrail, please visit datagrail.io or follow DataGrail on Twitter and LinkedIn.

DATAGRAIL®

To learn more, please visit **datagrail.io** or follow DataGrail on **Twitter** and **LinkedIn**