wirewheel

5 Key Steps

TO MANAGING

Subject Rights Requests

INSIDE YOU'LL LEARN:

1

WHY SUBJECT RIGHTS REQUESTS ARE CRITICAL TO DATA PRIVACY COMPLIANCE

Learn the rewards of getting it right and risks of getting it wrong

2

CCPA'S UNIQUE APPROACH TO SUBJECT RIGHTS REQUESTS

Understand the key differences between CCPA and GDPR

3

STEPS TO SUCCESSFULLY MANAGING SUBJECT RIGHTS REQUESTS

Overcome challenges to make your process transparent, efficient and compliant

EXECUTIVE OVERVIEW

One of the most fundamental and most challenging requirements within the California Consumer Privacy Act (CCPA) is the issue of Subject Rights Requests (SRR). As CCPA becomes operative in 2020, many businesses are expecting an influx of requests and worry that their current process isn't built for the scale and scope needed.

SRRs must be managed efficiently and securely to avoid significant financial and business risk. Preparing for SRRs under CCPA must be a collaborative effort among data privacy officers, information technology teams, and business leaders.

This eBook provides a framework for SRRs that balances individual rights provided under CCPA with the realities businesses face when working to satisfy them. You can use this framework as a decision-making tool as you create your SRR process. What's more, having SRR requirements in mind can also guide how you select services and vendors, develop products, and make choices about personal data you collect and use.

Subject Rights Requests are critical to data privacy compliance

Learn the rewards of getting it right and risks of getting it wrong

WHAT ARE SUBJECT RIGHTS REQUESTS?

Data privacy laws give people rights to access, change and control the data businesses collect about them. People make their wishes known to businesses in the form of a Subject Rights Request (SRR). The laws also require that businesses provide methods for people to register these requests and to respond accordingly.

"Subject Rights Request" is an umbrella term for this process, used without indicating specific regulations. Various privacy regulations use slightly different terminology and indicate different requirements. For example, GDPR uses the term Data Subject Access Requests (DSAR), as a "data subject" is any person whose personal data is being collected, held or processed. CCPA, on the other hand, uses the term Verifiable Consumer Request (VCR) to differentiate from GDPR.

Your business may need to comply with GDPR, CCPA, or any number of national or state-based data privacy laws that are being developed. In this eBook we'll conduct a deep dive into the requirements of CCPA, but the SRR framework can be applied to meet the requirements of any law that may come your way.

"Security and risk management leaders must carefully plan for subject rights requests as they affect every system and process involved in handling personal data."

– GARTNER RESEARCH[1]

THE SRRS YOU MAY RECEIVE FALL INTO THREE CATEGORIES:

The right to know

The most common type of SRR involves people seeking to know what data your organization holds about them and your intentions for collecting and using that data. They're requesting access to information, which is why these types of requests are commonly called Subject Access Requests (SAR).

The right to correct

People have the right to correct their data or their data preferences, including the "right to be forgotten" (to have an organization erase their records). These requests are often the most complex types of SRRs to address, as you must make sure any record deletion is completed throughout your data stores in a permanent way.

Right to object

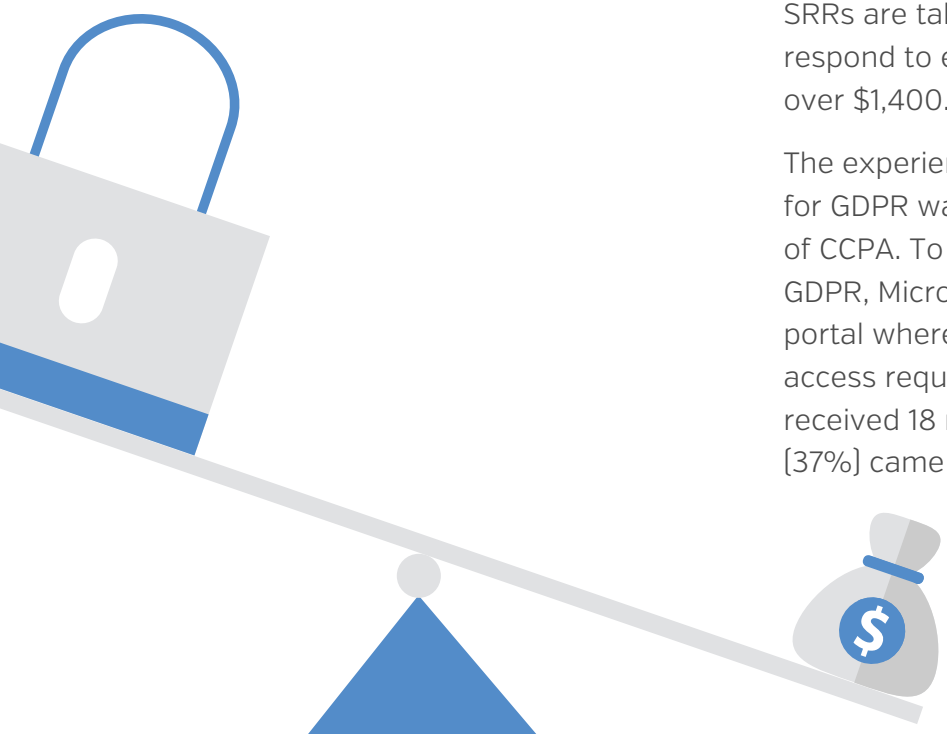
These types of SRRs involve granular control over how personal data is processed. For example, under CCPA, people may object specifically to the sale of their data to a third party.

SRR AS PART OF THE PRIVACY EXPERIENCE

Your business's approach to Subject Rights Requests is a critical part of the data privacy experience you create for your customers. Every external touchpoint within your SRR process should be communicated transparently, so your customers understand the process and feel their needs are being considered. Done well, SRRs can become a competitive advantage that builds trust and brand equity.

To achieve this level of excellence requires intentional planning and systems management.

The Risk of Getting it Wrong



FINANCIAL IMPACT OF SRRS ON BUSINESS OPERATIONS

SRRs represent a major challenge for businesses, with the potential to become an even greater hardship as CCPA and other regulations open the floodgates for thousands, or even millions of SRRs.

By 2021, 80% of the negative financial impact of the CCPA will come from failure to implement a scalable subject rights workflow, according to Gartner Research. Gartner found that today – before CCPA even comes into effect – the majority of organizations receiving SRRs are taking a full working week to respond to each, at an average cost of over $1,400.[2]

The experience of companies preparing for GDPR warns of the impending impact of CCPA. To address requirements of GDPR, Microsoft launched a self-service portal where customers could register access requests. In the first year, it received 18 million requests and 6.7M (37%) came from the United States.[3]

THE MORE CONSUMER DATA YOU COLLECT, THE GREATER THE CHALLENGE

For B2C companies in particular, the scope of Subject Rights Requests and the associated risk is sky high. With the power of modern marketing technology, B2C companies are tracking tons of data about known customers AND unknown users or prospective customers.

For most companies, data stores are typically a mix of first-party data from different business units and acquired companies, as well as behavioral insights, purchased data, and other third-party data from vendors that could fall under the requirements for SRRs.

For a company with fragmented records management, handling Subject Rights Requests can become very costly. Privacy and IT teams could spend valuable resources fulfilling data requests instead of focusing on priority projects.

Potential for CCPA fines and litigation

If you can't demonstrate a sufficient SRR process, under CCPA your business can be found non-compliant and penalized.

Again, the experience of businesses regulated under GDPR provides an indication of the potential impact of CCPA. In the United Kingdom, 46% of data protection-related complaints lodged with the Information Commissioner's Office are related to SRRs.

Under CCPA, fines are enforced by the Attorney General and can reach up to $7,500 per every violation (in the case of intentional violations). Non-intentional violations are subject to a $2,500 maximum fine.

In worst-case scenario, mistakes in the SRR process – even unintentional ones – can cause a data breach. A data breach opens the possibility of a private right of action under CCPA, which will exponentially increase your risk and financial liability. With damages in individual or class-action lawsuits ranging between $100 and $750 per violation, costs could escalate quickly.

$7,500

in fines for every intentional violation

$2,500

in fines per every non-intentional violation

+

$100 – $750

in damages awarded in individual or class-action lawsuits, per violation

2 CCPA's unique approach to Subject Rights Requests

Understand the key differences between CCPA and GDPR

CCPA expands consumer rights to include the following:

- To know *whether* personal data is collected about them.
- To know *what* personal data is being collected about them.
- To know specific *categories of data* a business collects about them.
- To know *categories of third parties* with whom personal data is shared.
- To know *categories of sources* of personal data.
- To know the *business or commercial purpose* of collecting personal information.
- To *correct* information about themselves.
- To *port* (move) their personal data.
- To say no to the *sale* (broadly defined as sale or exchange) of their personal data.
- To *delete* their personal data.

These requirements apply to both customers and non-customers.

Key differences between CCPA and GDPR's approach to Subject Rights Requests

You'll be obligated to comply with CCPA if you have $25 million in annual gross profits, if 50,000+ consumers, households or devices have personal information you buy, receive, sell or share, or if you derive more than half of your annual revenue from selling consumers' personal information.

CCPA isn't simply a U.S. version of GDPR. If you've already prepared for GDPR, you won't have to start over to prepare for CCPA, but that doesn't mean you have all the bases covered.

CCPA has additional requirements and is more prescriptive than GDPR. Even if your organization has already prepared diligently for GDPR, you'll need to revisit the process you have in place to handle Subject Rights Requests under CCPA as the two laws have overlapping requirements but distinct differences.

Below are the major differences between the two laws that impact how you handle Subject Rights Requests.

SCOPE

GDPR

Protects individuals within the EU and applies outside of the EU when a company sells products or services to individuals inside the EU or when individuals are targeted or monitored.

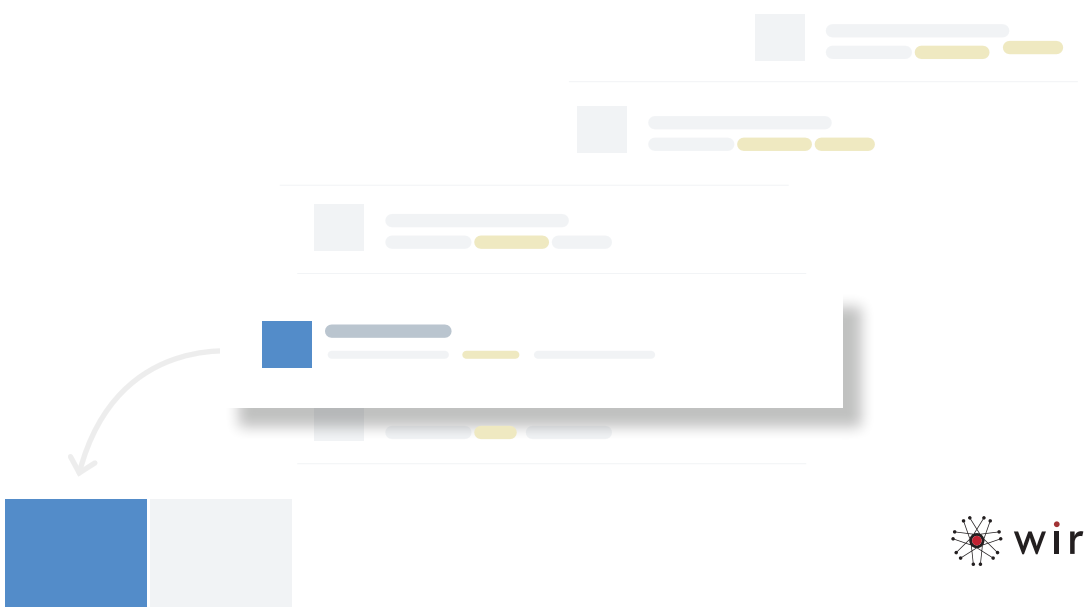
Covers “processing” of personal data, defined to include any operation performed on personal data, including collection.

VS

CCPA

Protects consumers who are residents of California, including households.

Covers collection, processing, as well as the sale of personal information.



DEFINITION OF PERSONAL INFORMATION

GDPR

Addresses personal data, defined as any information relating to an identified or identifiable natural person (data subject), including publicly available data.

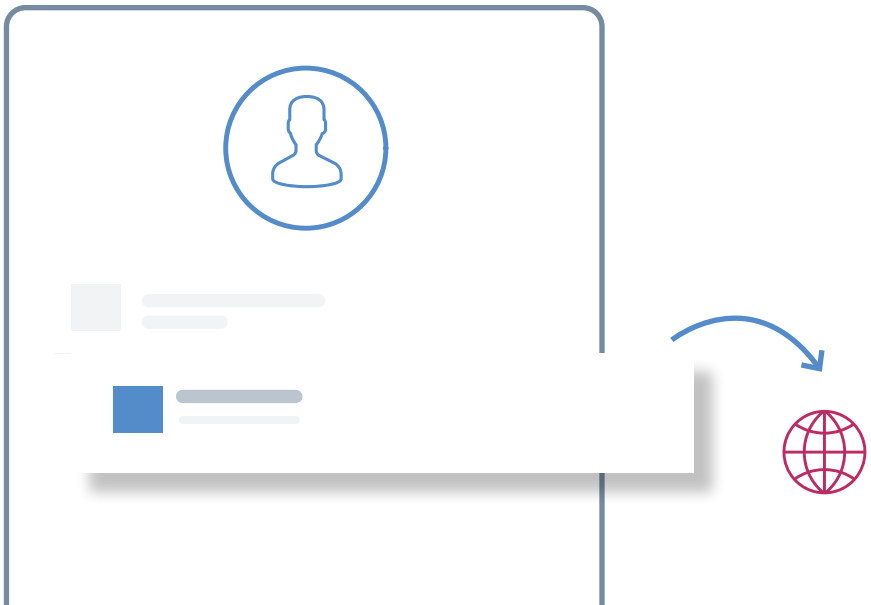
(Doesn't apply to anonymized data).

VS

CCPA

Addresses information that relates to, describes, is capable of being associated with, or could reasonably be linked, indirectly or directly, with a consumer or household.

Doesn't apply to deidentified data (i.e., data that can't be reasonably linked with a consumer or household), or aggregate data that can't be linked to a consumer or household.



RIGHT TO ACCESS

Data subjects have the right to request access to their personal data.

They must provide the personal data undergoing processing.

VS

Consumers have the rights to know:

- whether personal data is collected about them.
- what personal data is being collected about them.
- specific categories of data a business collects about them.
- purposes for which information has been or may be used.

Disclosure includes data covered 12 months before request.

RIGHT TO ERASURE/DELETION

Individuals have the right to erasure of their personal data.

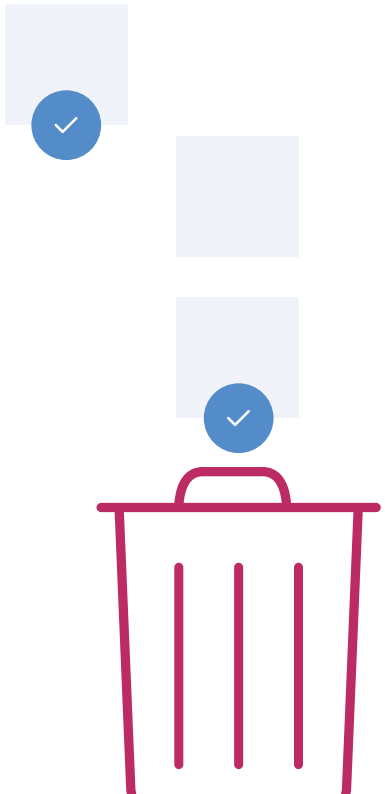
If the controller has made the personal data public, it must take reasonable steps to inform others that are processing the data that the data subject has requested erasure and must inform the data subject about those steps upon request.

Applies to all data concerning a data subject.

Except when it is necessary:

1. for exercising the right of freedom of expression and information.
2. for compliance with an EU or Member State legal obligation.
3. for reasons of public health and medicine.
4. for archiving, scientific or historical research, or statistical purposes, subject to minimization (e.g., pseudonymization).

VS



Consumers have the right to deletion of their personal information.

Applies only to data collected from the consumer (i.e. not to data about the consumer collected from third party sources).

Except when it is necessary to:

1. Complete the transaction for which the information was provided or perform a contract with the consumer.
2. Detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity and prosecute those.
3. Debug to identify and repair errors that impair existing intended functionality.
4. Exercise free speech (of business or another consumer) or other rights.

RIGHT TO PORTABILITY

A data subject has rights to:

- receive a copy of their personal data in a structured, commonly used, machine-readable format; and
- transmit the data to another controller without hindrance from the original controller, including to have the personal data transmitted directly from the first controller to the second controller.

VS

Disclosures must be delivered by mail or electronically. If delivered electronically, information must be portable and in a readily useable format.

TIMING AND FORMAT

Controllers and processors must know how to identify a request.

If the request has been requested electronically, data must be provided electronically.

Data subject's requests must be complied with within one month from receipt of request. Businesses can extend two months if they notify the data subject.

VS

Businesses must disclose within 45 days of receipt of "verifiable request."

Business may exercise one 45-day extension when reasonably necessary if they notify the consumer within the first 45-day period.

For more background on CCPA, download The Ultimate Guide to California's Data Privacy Law.

For a full list of key differences between GDPR and CCPA, get our cheat sheet.

Steps to successfully managing Subject Rights Requests

Overcome challenges to make your process transparent, efficient and compliant

The better you manage Subject Rights Requests, the better the privacy experience will be for your customers, the easier the effort will be for your internal team, and the more likely you are to meet the expectations of auditors and regulators.

Below are five critical steps to build an efficient, compliant SRR process, including some "gotchas" to avoid.

STEP 1. Verify and authenticate requests

If you receive a request for information on a person's data, you need to confirm the person's authority to make the request. IAPP recently warned about the risk of fake requests leading to data breaches.[4] The last thing you want is to provide personal, protected information to the wrong person.

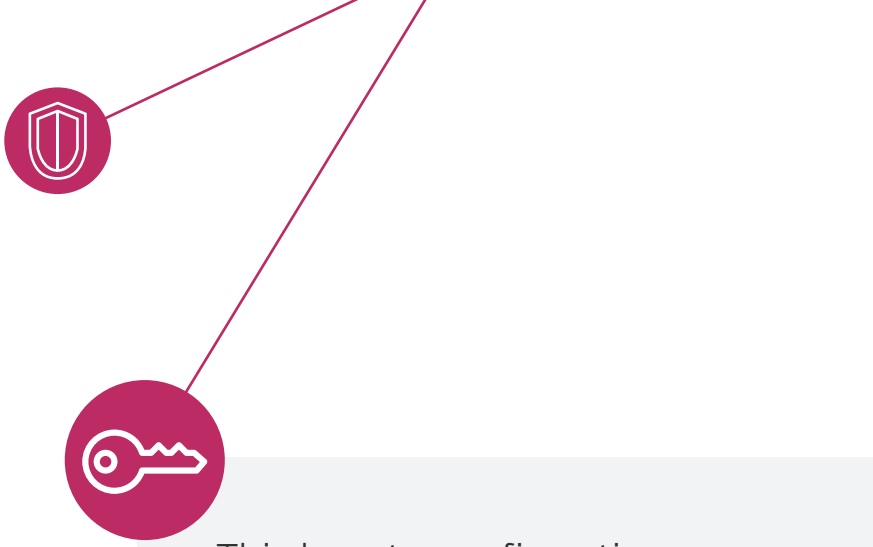
Gartner recommends the confirmation process "should be proportionate to the impact of the request." For example, Gartner says, "if the person wants to restrict one or two preferences, a username/password or a few challenge questions on the phone

may be sufficient. However, if individuals want to download a decade worth of detailed personal data or delete their accounts, then this may necessitate stronger identity verification."[5]

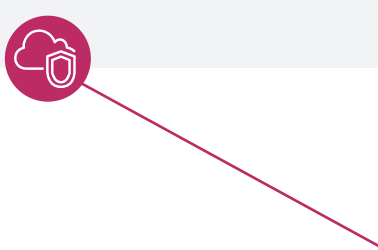
If your customers already have password-protected accounts, you can confidently match the person making the request to a specific individual. But, if a Subject Rights Request comes from an unknown user, confirming who they are and their right to the information is trickier, for several reasons:

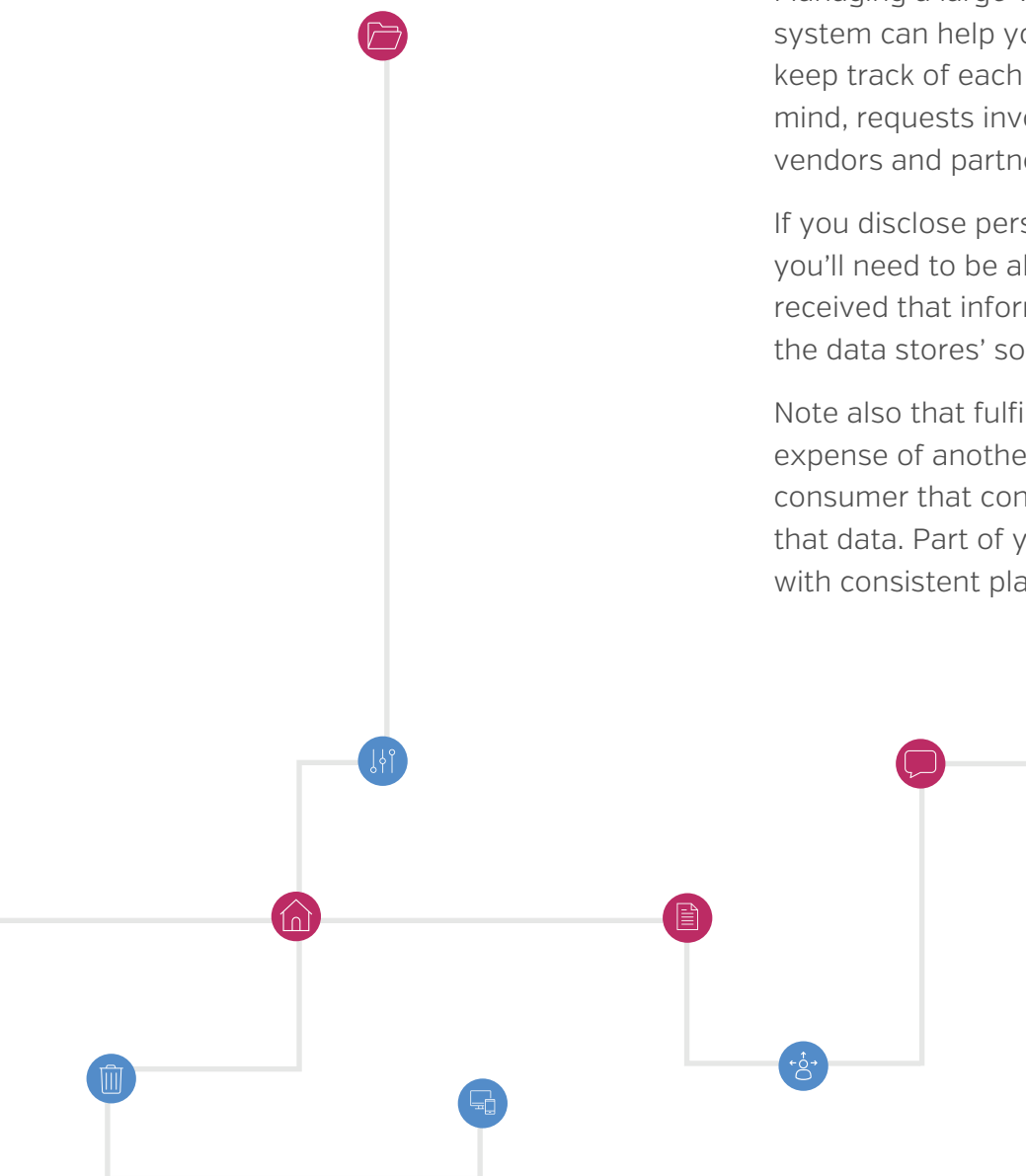
- Consumers may not be making requests themselves. Parents may request data on behalf of their minor children or other individuals may be authorized to act on their behalf. Consider a parent wanting to know the history of their son's personal data collected or shared via an online game.
- Multiple users may be sharing a device, so relying on device data is not sufficient to confirm individual identity. Consider a husband and wife sharing an account for the household.
- You aren't allowed to ask for any additional personal information from the consumer than what you've already got. Doing so constitutes a data breach and increases your liability. Requiring users to provide a copy of ID document, passport or other official, government-issued document, such as a birth certificate, isn't allowed.

You're caught between a rock and a hard place. You can't say no to all Subject Rights Requests and you can't answer them all without more information. This is where a third-party can provide verification and authentication to remove the burden.



Third-party confirmation involves "verification" – making sure any asset, such as a document or email address a person provides is legitimate – and "authentication" – making sure that asset is tied specifically to that individual.





STEP 2. Set up a system to process requests across your data supply chain

Managing a large volume of Subject Rights Requests is a team sport. A ticketing system can help you assign requests, or parts of requests, to different people and keep track of each task as the request progresses through your workflow. Keep in mind, requests involve not only team members within your organization, but also all vendors and partners with whom you shared personal information.

If you disclose personal information to third parties, such as vendors or partners, you'll need to be able to send a deletion request to all of the downstream parties who received that information. Even more challenging, you must be able to track back to the data stores' sources and request that the personal information has been deleted.

Note also that fulfilling one person's Subject Rights Request shouldn't come at the expense of another's right to privacy. For example, beware of sending data to a consumer that contains names and/or emails of staff members involved in collecting that data. Part of your process should include flagging and replacing identifiable data with consistent placeholders (i.e. replacing "John Smith," for example, with ".")

"Simply put, if you are not able to identify and monitor where an individual's information resides and how it is used, you will not be able to produce it and you will also not be able to modify it – a requirement for updates, erasures or maintaining adequate management procedures."

– GARTNER[6]

STEP 3. Collect data to address requests

Responding to a Subject Rights Request (SRR) typically requires accessing, modifying, and possibly deleting, data from the backend data management systems that are hosting personal data.

Most companies have vast file repositories which often reside in silos. Customer data may be inside CRM systems, marketing databases, product databases, customer care logs, or other repositories. Employee data may live in HR, financial or healthcare systems.

In a typical enterprise, these data stores include structured relational (SQL) databases (e.g., PostgreSQL, Oracle, SAP, MS SQL Server) or semi-structured databases (e.g., MongoDB, Azure CosmosDB, AWS DynamoDB), which typically serve as backends of operational or production processes; data warehouses like Snowflake, Oracle Exadata, Teradata, SAP, etc., that typically serve as the backend of data analytics and machine learning processes; file systems and file shares (e.g., Google Drive, SharePoint); data lakes; CRMs; Enterprise Service Busses (ESBs); and others. For deletion and correction requests, backups, and offline data stores may also be involved.

To identify related files across all systems, you need the capacity to index data and apply relevant metadata to information so it's trackable and searchable. The faster you can query your data stores automatically, the easier the SRR process will be.

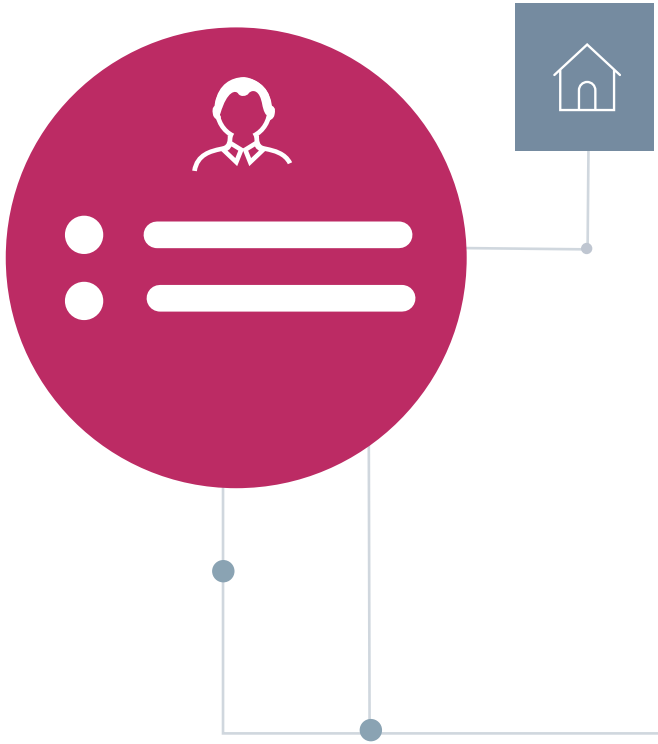
Manual collection at the scale, speed, and accuracy required for SRRs is virtually impossible. To have that level of granular supervision and control, you need an automatic way to log, classify, and validate repositories of personal data that may be subject to SRRs.

STEP 4. **Deliver information securely to customers**

The way you provide information in response to requests is another part of the SRR process you must handle with care to avoid a data breach. Only the sender of a request should be able to receive the data in return.

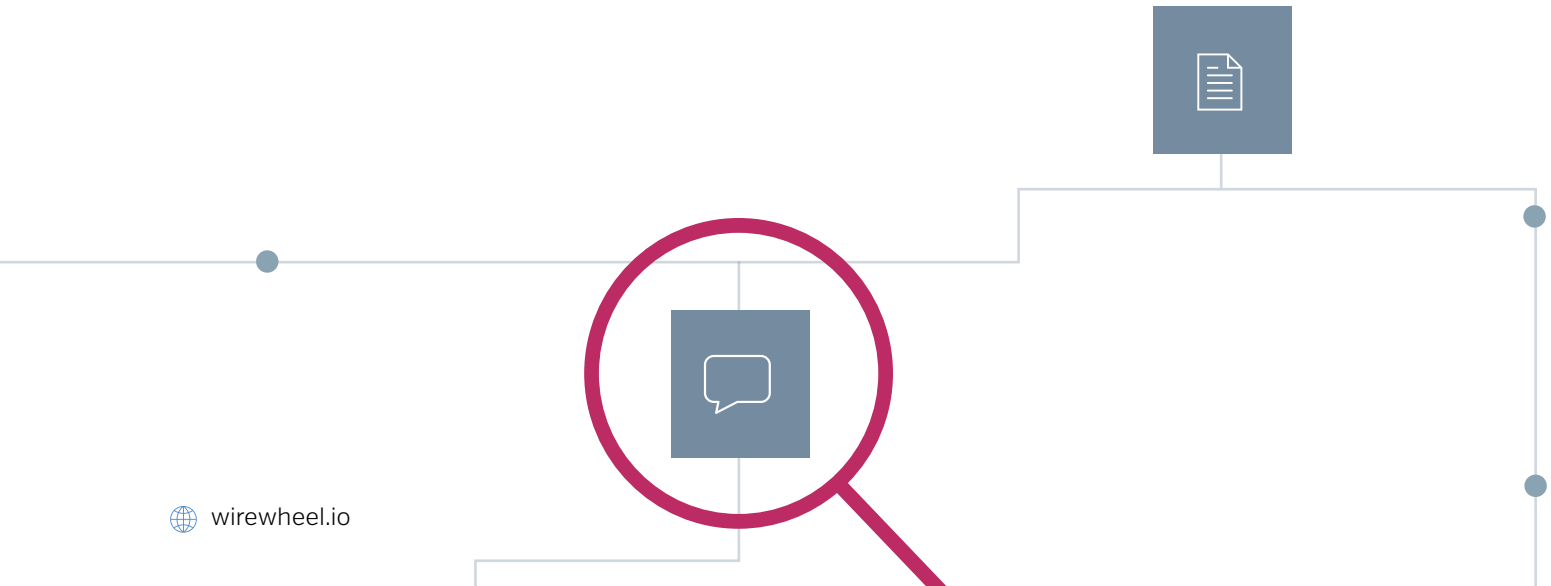
When starting to manage consumer requests, it can be tempting to use existing systems, like email or content management systems [such as SharePoint or Dropbox. But, passing information via unencrypted systems may expose you to a data breach, which, as we've discussed, dramatically increases your liability.

Therefore, you should make sure consumer information is sent securely, encrypted at rest and in-transit, all the way from request to delivery.



STEP 5. **Document your process for tracking, reviewing and approving requests**

You can demonstrate compliance with privacy laws by recording all communications, reviews, and approvals that are part of your SRR process. You should maintain complete audit trails of all the requests you receive and actions you take so that when an auditor asks, you have them at the ready.

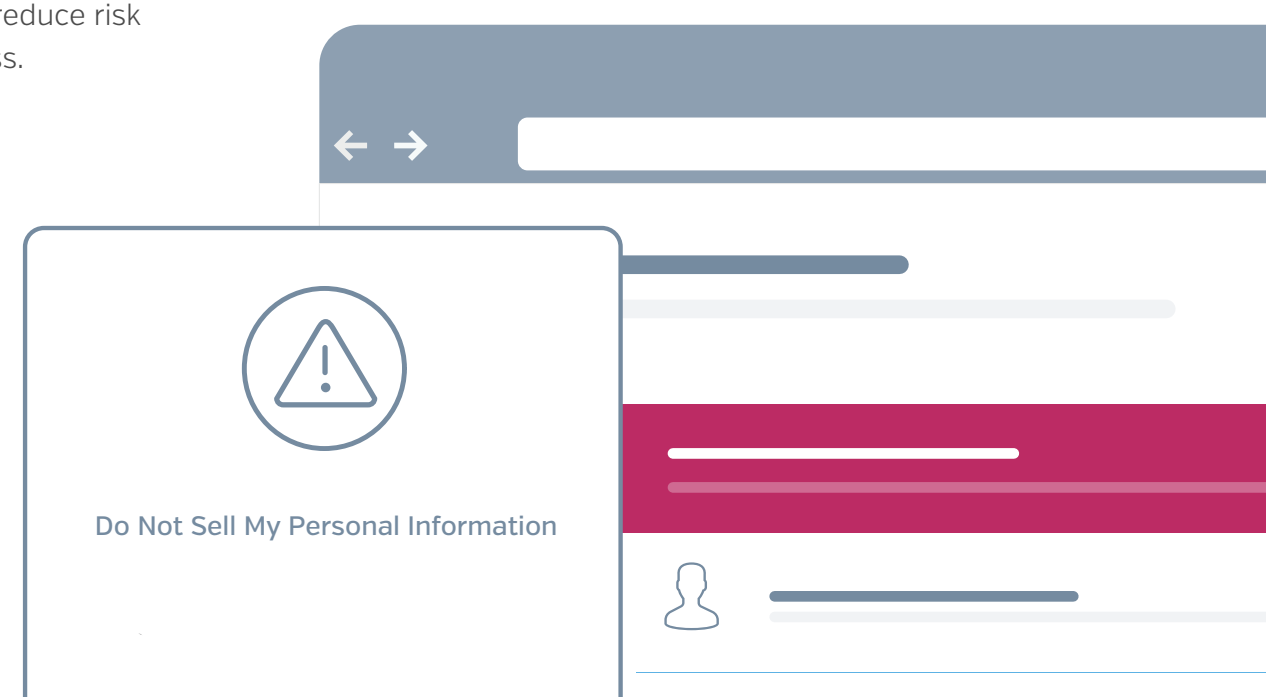


Conclusion

If your business collects or processes personal data of residents of California, you should be building, documenting and testing your SRR process now.

Even if CCPA doesn't directly apply to your business at this point, the law is raising the bar for all data privacy regulations and is an indication of requirements you will also need to meet.

Following the recommendations outlined for an efficient, secure SRR process will help you create a data privacy experience you'll be proud to share with consumers, including current customers and those you hope will become customers. You'll reduce risk and save valuable time and resources in the process.



How WireWheel can help

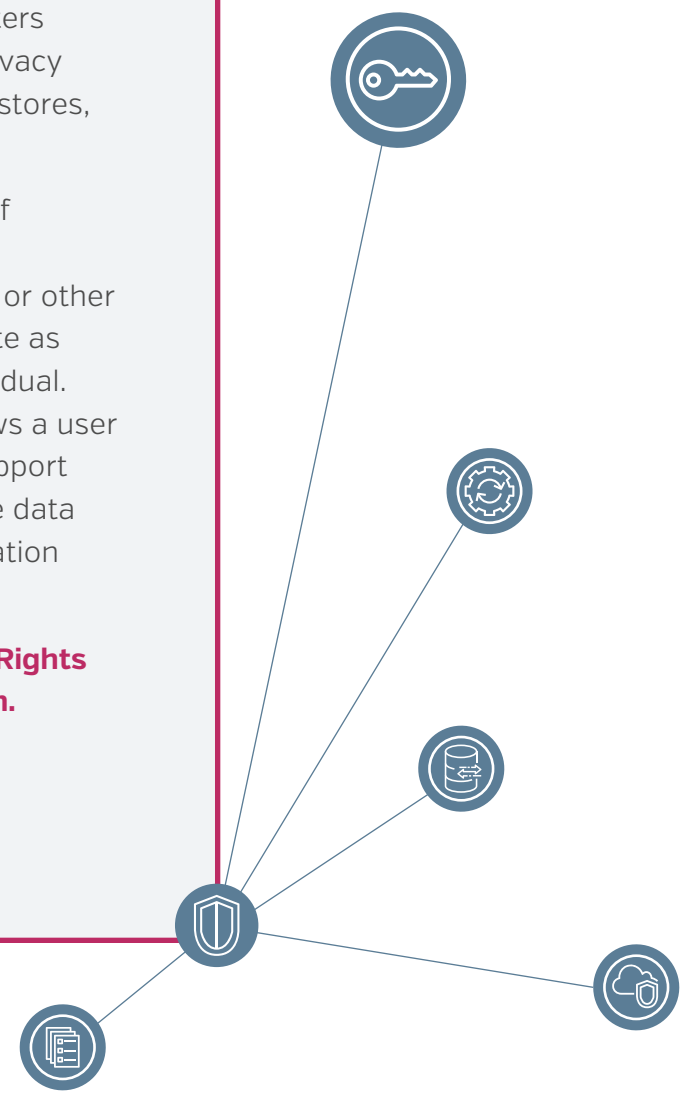
Schedule a Demo!
www.wirewheel.io/demo

WireWheel's consumer-facing portal gives you the capability to receive Subject Rights Requests (SRR), whether requesters are known customers or unknown individuals. Our data privacy management platform helps you assign tasks, query data stores, and identify specific consumer data to respond to SRRs.

Most importantly, WireWheel solves the twin challenges of verification and authentication. As a third-party provider, WireWheel helps you verify that an email, driver's license, or other asset a consumer provides as proof of identity is legitimate as well as authenticate that it's connected to a specific individual. An additional option for an electronic sworn affidavit allows a user to certify their identity, giving you a legal document to support your SRR activity. Our encrypted environment secures the data and we never use data for any purpose other than verification and authentication of your company's SRRs.

We'd love to show you how WireWheel enables Subject Rights Requests. Get in touch for a personalized demonstration.

wirewheel



About WireWheel

The WireWheel team is comprised of privacy experts, data scientists, cloud ninjas, PhDs, policy wonks and others who care deeply about data, privacy and building trust in the digital era.

WireWheel's Privacy Management Platform equips privacy, security and IT professionals to quickly answer the four central questions at the heart of any privacy initiative: what data you have, why you have it, where that data is stored and processed, and who you are sharing that data with and for what purpose.

WireWheel's platform helps organizations comply with today's CCPA and GDPR requirements while remaining ready for any future regulatory regimes, minimizing legal risks and reducing the time and effort it takes to respond to various types of data subject requests.

Resources

[1] Gartner Research, “Practical Privacy – Executing Subject Rights Requests,” July 2018

[2] Gartner Research, “How to Prepare for the CCPA and Navigate Consumer Privacy Rights,” June 2019

[3] “GDPR’s First Anniversary: A Year of Progress in Privacy Protection,” Microsoft Blog

[4] https://iapp.org/news/a/fake-dsars-theyre-a-thing/

[5] Gartner Research, “Practical Privacy – Executing Subject Rights Requests,” July 2018

[6] Gartner Research, “Practical Privacy – Executing Subject Rights Requests,” July 2018

Disclaimer

wirewheel