

Managing Subject Rights Requests at Scale: Five Tips from Microsoft to Automate your SRRs



Contents

01 /

Contents

02 /

Executive summary

03 /

Regulatory landscape and
requirements for subject
rights requests

Challenges of managing
subject rights requests

Strategies to make subject
rights request management
efficient and effective

04 /

Tip 1: Automate data
discovery and retrieval

05 /

Tip 2: Integrate with your
information security and
compliance solutions

Tip 3: Take advantage of
a robust triage
and review platform

06 /

Tip 4: Ensure secure and
compliant collaboration

07 /

Tip 5: Choose a solution
compatible with your
existing privacy ecosystem

Microsoft Priva Subject
Rights Requests: Supporting
a more efficient strategy

08 /

Get started today

Executive summary

Data privacy regulations—such as the European Union’s General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA), and Brazil’s Lei Geral de Proteção de Dados (LGPD)—grant consumers the right to request what specific data organizations have collected about them. With consumers seeking more control over their data, responding to subject rights requests (SRRs) is an important topic for many organizations. However, fulfilling these requests can be a manual and cumbersome process.

As someone concerned with security and privacy for your organization, you need a well-defined strategy that makes managing SRRs more efficient. In this e-book, we’ll share five tips to automate your SRRs, enabling you to manage the increasing number of requests at scale. Additionally, you’ll learn about how Microsoft Priva Subject Rights Requests can help you on this journey in implementing these tips.



Regulatory landscape and requirements for subject rights requests

Consumers are seeking greater control of their personal data. They're empowered by recent data privacy regulations—such as the European Union's General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA), and Brazil's Lei Geral de Proteção de Dados (LGPD)—that have introduced the fundamental right to understand what information an organization has collected and the right to remove that information if requested. An SRR enables a customer or employee (that is, the data subject) to request, review, and manage the personal data that companies have collected about them and request the erasure, rectification, cancellation, opposition, or portability of their data.

When a consumer exercises a rights request, organizations need to accurately and efficiently find all data associated with an individual's name and provide a detailed report to the subject in a specific timeframe.



Challenges of managing subject rights requests

Managing SRRs is time-consuming and costly, especially when it comes to unstructured data like emails, messages, and documents. Organizations store large amounts of personal information but don't have easy ways to conduct searches and review data outside of a relational database.

According to a recent Gartner® survey, most organizations are processing between 51 and 100 subject rights requests (SRRs) per month, with the processing of a single access request costing more than \$1,500.

[Gartner Market Guide for Subject Rights Request Automation.](#)
[November 2021.](#)

Even though some organizations automate personal data discovery, the complexity and sensitivity of handling SRRs still require manual review and collaboration that results in high costs and intensive resources. For example, once identifying files containing personal data, a manual process is often required to review each item to ensure no other data subject's confidential information would be shared in the same file or reveal information that cannot be shared. Then, they must collaborate with multiple stakeholders, sometimes in a not secure or compliant way. Inefficient, untimely, and non-compliant handling of SRRs can result in financial penalties, loss of consumer trust, and significant reputational damage.

Strategies to make subject rights request management efficient and effective

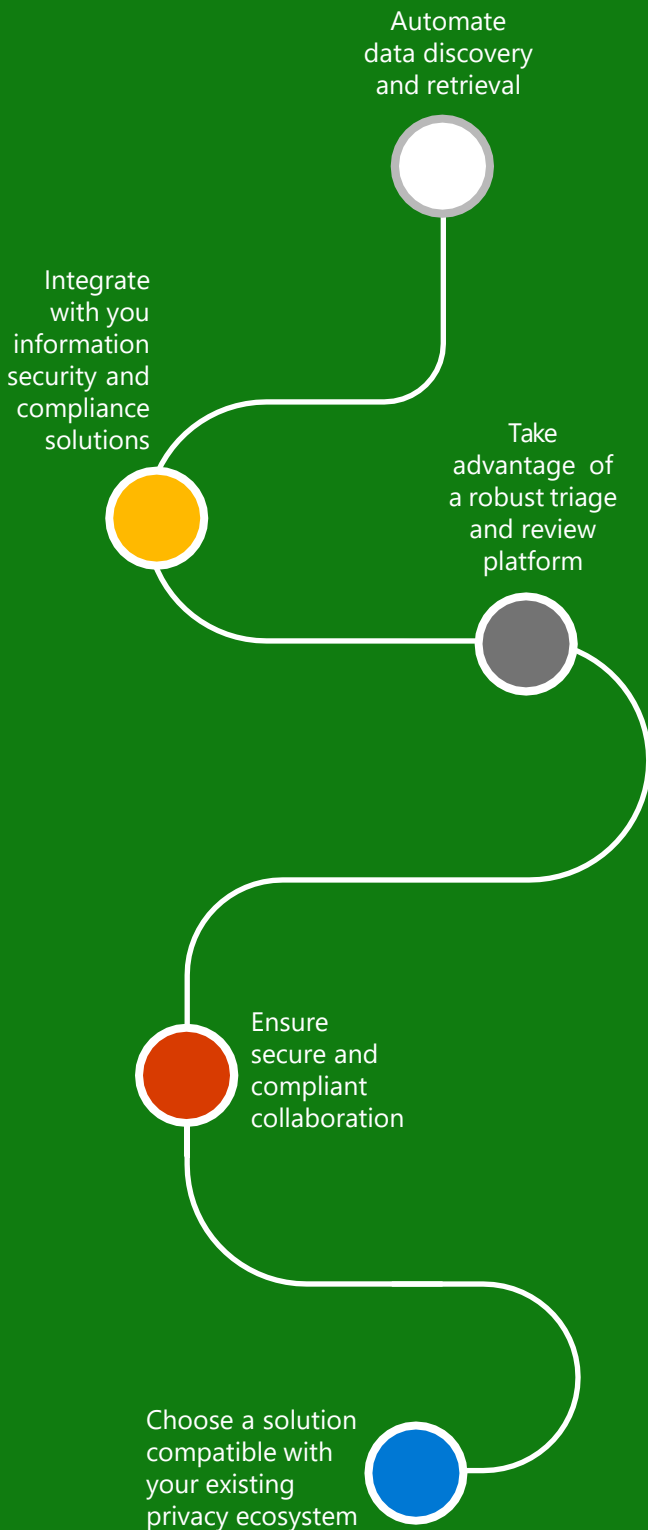
A more strategic approach can help you overcome these challenges. You can start by focusing on a standardized and integrated process to support SRRs management. That process begins with finding relevant data, identifying data conflicts, triaging multi-person data and legal conflicts, and finally reviewing the data set across multiple teams before responding to the subject's request.

To find a path forward, it's worth considering these five tips in managing and responding to SRRs:



5 tips

Learn
about how
Microsoft
Priva Subject
Rights Requests
can help you on
this journey in
implementing
these tips.



Tip 1: Automate data discovery and retrieval

The first and most important step in responding to an SRR is finding the subject's data. For that, you need the right tool for the right task. While sophisticated legal tools are useful to automate data discovery for litigations and investigations, SRRs require a more intuitive user experience to allow broader use across your organization and a quick turnaround time. A simple, straightforward tool—specifically designed with your SRRs process in mind— allows more people in your organization to take advantage of the automated data discovery.

The faster and easier you can search for data, estimate data volume, and adjust search queries, the more efficient your SRRs process will be. Once you finalize the search criteria, such as full names, email, phone numbers, or other more sensitive personal information, the system should automatically scan through the environments you specified and gather the data set for review.



Microsoft Priva Subject Rights Requests (Priva SRRs) make it easy to define search criteria and the scope of your data search and automatically collect the data set for your review.

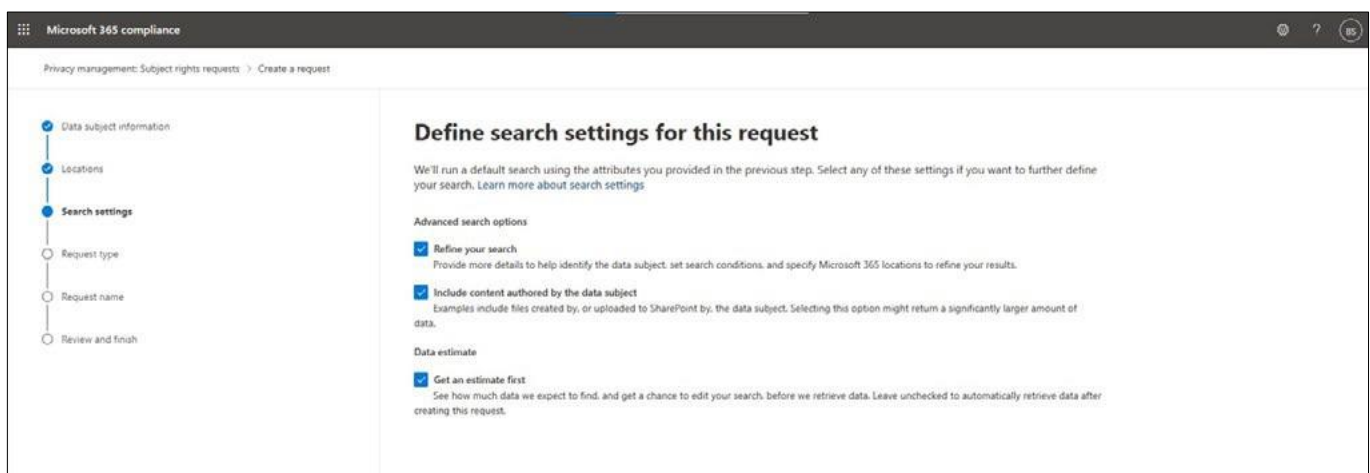


Figure 1. Easily define your search settings in Priva SRRs

Tip 2: Integrate with your information security and compliance solutions

Automating the discovery of personal data isn't enough; you need further visibility into the context and risks associated with the data. For example, when responding to SRRs, you may want to know whether the file is on legal hold, contains confidential information, or includes multiple people's personal information. To identify data conflicts, you must review each document and might need to cross-check different platforms manually.

Integrating the SRRs tool with your information security and compliance solutions could help identify potential data conflicts more efficiently and with greater accuracy.



Priva SRRs automatically detect data conflicts to subject requests, including legal holds, confidentiality, and multiple people's personal data.

The screenshot shows the Microsoft 365 compliance center interface. The left sidebar contains navigation options like Home, Compliance Manager, Data classification, Data connectors, Alerts, Reports, Policies, Permissions, Trials, and Solutions. The main area displays a Subject Rights Request (SRR) for Akira Jennings, titled 'Akira Jennings - Access'. The request is at Stage 3 of 5 - Review data. The interface shows a list of items with columns for Item name, Review status, Tags, and Content owner. A detailed view of a selected item, '9-19 Spartan Background Check.xlsx', is shown on the right, including source, plain text, and details like content owner, location, and tags.

Item name	Review status	Tags	Content owner
Empty subject	Not reviewed	Not tagged	N/A
9-20 Spartan Background Chec...	Not reviewed	Not tagged	a.abbot035
Empty subject	Not reviewed	Not tagged	N/A
The new Akira Jennings - Acc...	Not reviewed	Not tagged	Akira Jenning...
Empty subject	Not reviewed	Not tagged	N/A
Akira sent a message	Not reviewed	Not tagged	Akira Jenning...
9-19 Spartan Background Chec...	Not reviewed	Not tagged	c.george388
Welcome to your monthly dig...	Not reviewed	Not tagged	Microsoft Vm...
9-20 Spartan Background Chec...	Not reviewed	Not tagged	c.george388
The new Akira Jennings - Acc...	Not reviewed	Not tagged	Akira Jenning...
9-20 Spartan Background Chec...	Not reviewed	Not tagged	c.george388
9-20 Spartan Background Chec...	Not reviewed	Not tagged	c.george388
Akira sent a message	Not reviewed	Not tagged	Akira Jenning...
9-19 Spartan Background Chec...	Not reviewed	Not tagged	c.george388


Details for '9-19 Spartan Background Check.xlsx':

- Source: Plain text
- Annotate: Details
- File notes: Review status: Not reviewed
- Location: SharePoint
- Last modified: Sep 19, 2021 4:26 PM
- Tags: Follow-Up
- URL: https://tredev3-my.sharepoint.com/personal/c_george388_tredev3_com/microsoft_com/Documents/9-19 Spartan Background Check.xlsx
- Number of personal data found: 4
- Personal data found: tredev3@125, Credit Card Number, U.S. Social Security Number (SSN), All Full Names
- Priority types: TTE - Highly Confidential, Multi-person data

Figure 2. Identify critical data conflicts in Priva SRRs

For example, if the SRRs tool is integrated with your information protection solution, you can easily correlate the data signals across the two systems and find an individual's files that contains confidential information. The integration helps to prevent high-value business information from being shared with data subjects without appropriate processing or protection.



A man with a shaved head and a goatee, wearing a red t-shirt, is looking down at a tablet device. He is sitting at a table, and a yellow mug is visible in the foreground. The background is a warm, wooden wall.

Tip 3: Take advantage of a robust triage and review platform

After the subject data is compiled, you must review the findings, make choices about what to include, and redact information, as necessary. For example, suppose an individual's file also contains someone else's personal information. In that case, before you include the file in the response, you need to redact information that doesn't pertain to the person who made the request.

The review process can be manual and time-consuming, with reviewers sometimes only getting a list of file paths and metadata of the files containing personal data. In this situation, they would likely need to copy the file paths to the browser and review them one by one for verification.



Priva SRRs allows you to easily click on a file and conduct built-in reviews. All the metadata and user activities logs are in one view, so the reviewers can understand why the data was collected if a data subject raises a question.

Using a system that allows you to review a wide variety of file types in a single view can save you a tremendous amount of time when tagging files, making annotations, and redacting information. The system should automatically identify data conflicts, so reviewers can quickly understand the issues and take the right actions.

Microsoft 365 compliance

Privacy management: Subject rights requests > Akira Jennings - Access Jan 2022

Akira Jennings - Access Stage 3 of 5 - Review data

Overview Data collected Notes Collaborators Reports

Filter Reset Filters

Location: Any Review status: Any Tags: Any Content owner: Any

Item name	Review status	Tags	Content owner
9-20 Spartan Background Chec...	Included	Not tagged	a.abbott036
Empty subject	Not reviewed	Not tagged	N/A
Empty subject	Not reviewed	Not tagged	N/A
The new Akira Jennings - Ace...	Not reviewed	Not tagged	Akira Jenning...
Empty subject	Not reviewed	Not tagged	N/A
Akira sent a message	Not reviewed	Not tagged	Akira Jenning...
9-19 Spartan Background Chec...	Not reviewed	Not tagged	c.george388
Welcome to your monthly dige...	Not reviewed	Not tagged	Microsoft Viv...
9-20 Spartan Background Chec...	Not reviewed	Not tagged	c.george388
The new Akira Jennings - Ace...	Not reviewed	Not tagged	Akira Jenning...
9-20 Spartan Background Chec...	Not reviewed	Not tagged	c.george388
9-20 Spartan Background Chec...	Not reviewed	Not tagged	c.george388
Akira sent a message	Not reviewed	Not tagged	Akira Jenning...

1 of 56 selected

9-20 Spartan Background Check.xlsx

Source Plain text Annotate Details File notes

Redacted

SSN 016-35-5704 A.Jennings011@tredev3.onmicrosoft.com Akira Jennings

Redacted

Include Exclude Not a match Reset status Apply tags

Figure 3. Redact other personal data in the annotation view of the collected file in Priva SRRs



Tip 4: Ensure secure and compliant collaboration

It's critical to create a secure collaborative environment that allows various stakeholders to work together on SRRs. In the past, personal information was sent for review and approval over emails or messages to stakeholders, often creating more privacy and security concerns. When stakeholders collaborate on emails or messages during the review process, they create a more personal data footprint for that data subject, which can become a privacy and security risk if the communication isn't protected.

You need a centralized, secure, and compliant way for team members to collaborate, discuss, coordinate, and resolve issues as subject request responses are compiled.



Priva SRRs provides a centralized review platform and Microsoft Teams to help govern collaboration throughout the SRRs process. Additionally, you can set up protection, retention, and deletion policies for the collaboration content.

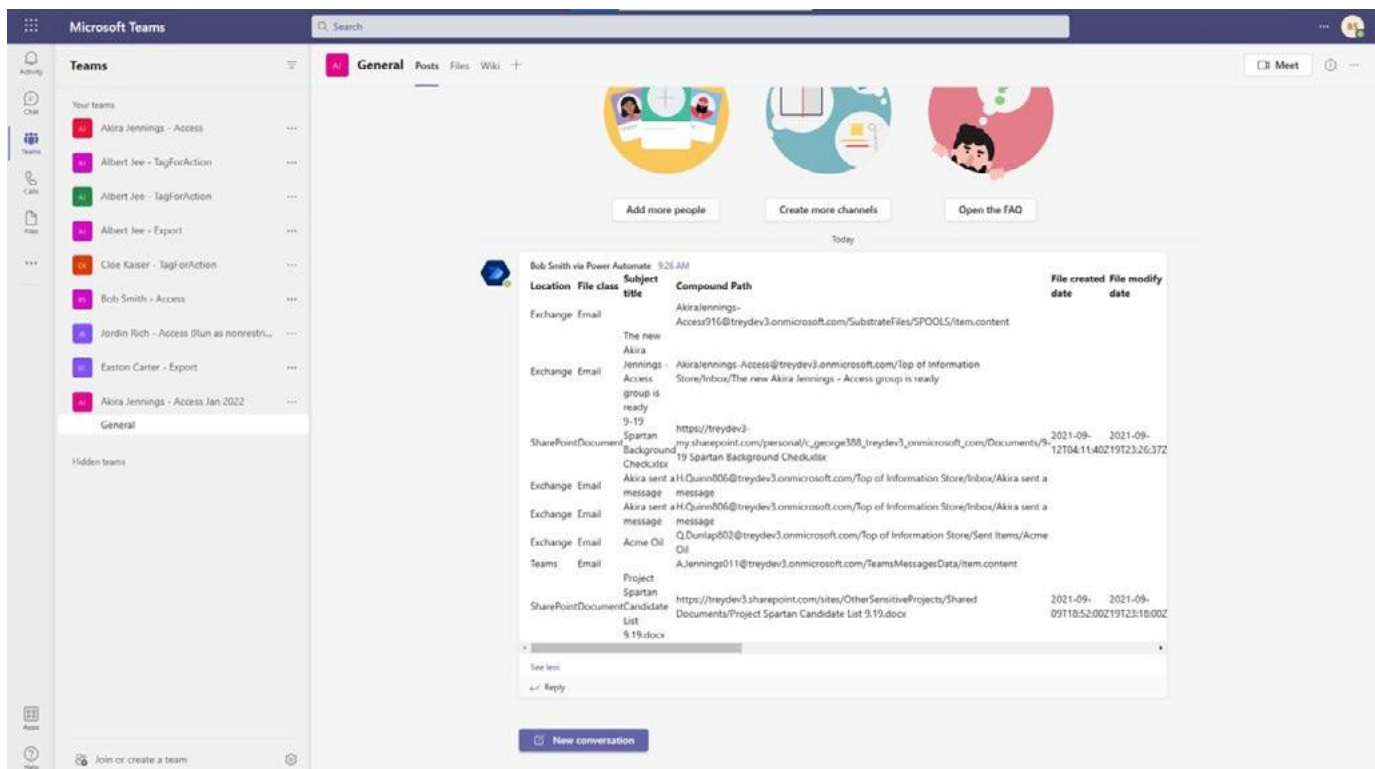


Figure 4. Secure collaboration around SRRs in Microsoft Teams

Tip 5: Choose a solution compatible with your existing privacy ecosystem

Most organizations use multiple solutions to manage privacy, with only four percent of companies using one end-to-end privacy management solution. Compatibility between solutions is essential to reduce implementation overhead and provides aggregated insights across solutions.

For example, if an organization uses an IT ticketing system to manage various privacy-related workflows, it will be ideal that the SRRs tool can also create and manage workflows in the same IT ticketing or workflow systems.



Microsoft Graph APIs for SRRs enable you to integrate Microsoft 365-related requests with your in-house or partner-built privacy solutions. This API-based extensibility enables you to respond to SRRs in a unified manner across your entire data estate, covering both Microsoft and non-Microsoft environments.

Priva SRRs also provide built-in Microsoft Power Automate templates that allow your admins to create a record for SRRs in ServiceNow or add other custom workflows.

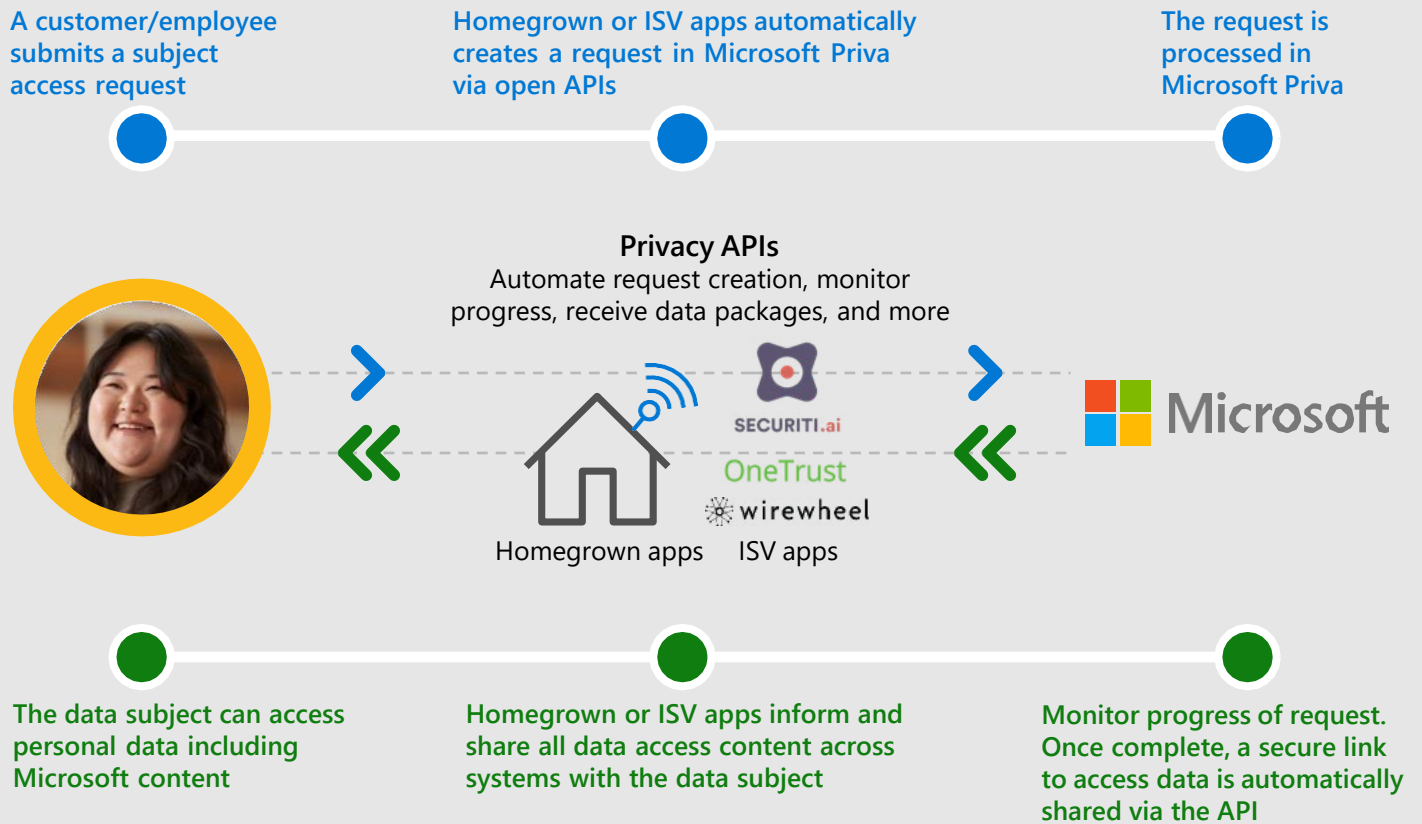


Figure 5. Priva SRRs integrates with other privacy management solutions



Microsoft Privacy Subject Rights Requests:

**Supporting a
more efficient
and streamlined
response
management**



With Priva SRRs, you can automate and manage SRRs at scale. Priva SRRs automatically find the subject's personal data, recognize data conflicts, and provide built-in review and redaction capabilities while enabling secure collaboration through Microsoft Teams. The solution can be integrated with your homegrown or partner-built privacy solutions, enabling you to have a unified and streamlined response to SRRs.

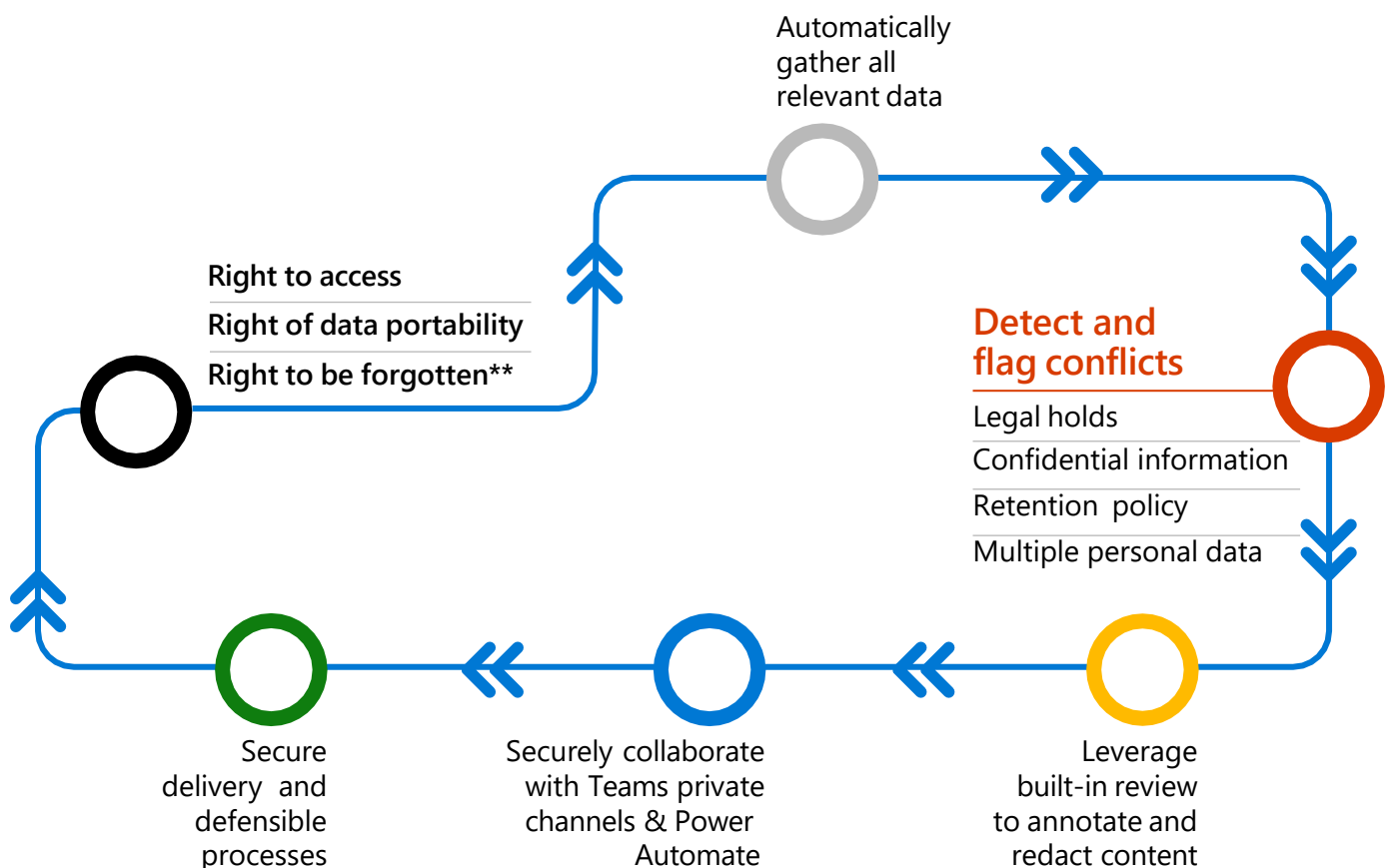


Figure 6: Priva SRRs provides automation and secure collaboration to fulfill subject right requests

**We provide a Power Automate template to help with custom actions

Start 90-day free trial

<https://aka.ms/trypriva>

Microsoft is excited to help ease the complexity of SRRs management. We hope the tips in this e-book lead you toward a more efficient method for completing and fulfilling requests. You can learn more about the solution in the [technical documentation](#) and [try out Priva Subject Rights Requests for 90 days](#) or create up to 50 subject rights requests (whichever limit expires first) at no cost.



Learn more about how Microsoft Priva can help you build a privacy-resilient workplace:

<https://aka.ms/priva/web>