

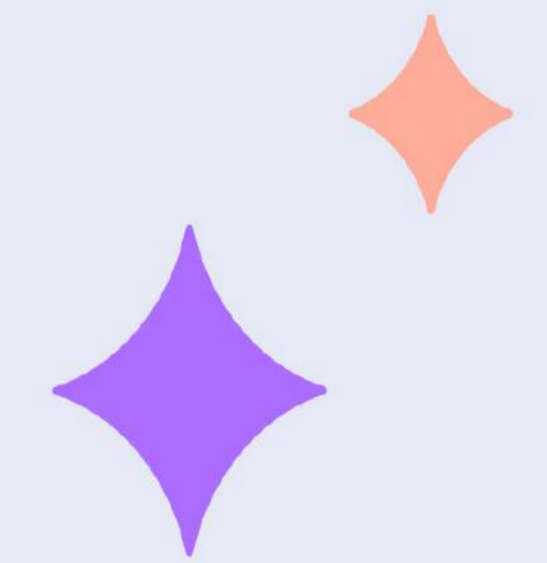
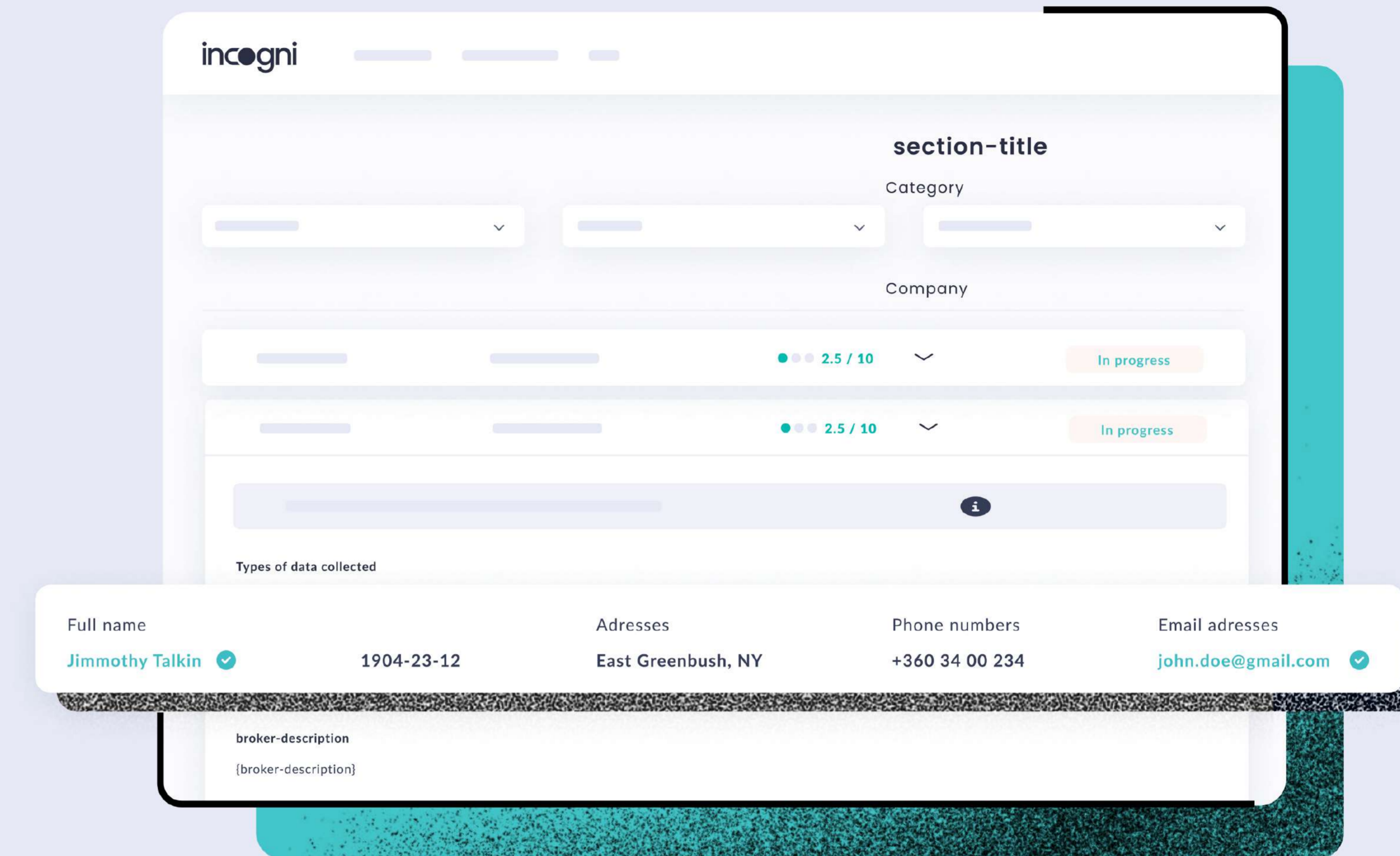
Incogni's Partner Guide

Incogni is a personal data removal service created by Surfshark that removes users' personal information from hundreds of data brokers' databases.

Data is a commodity in the internet age, with data brokers making money off of internet users' personal information. They buy and sell personal data such as **Social Security Numbers, contact details, and physical addresses.**

And the worst part? They usually do this **without informed consent.** Every time someone accepts cookies, downloads an app, or even just visits a website, data brokers may harvest their personal information.

We currently have hundreds of data brokers on our contact list and use the CCPA, UK-GDPR, GDPR, and PIPEDA to provide service to residents of the US, UK, EU, Switzerland, and Canada.



How Incogni works

Incogni offers an **automated** personal data removal service. We handle all interactions with data brokers, from **follow-up** communication to fighting rejected claims. We help our clients get their data deleted in a **fraction of the time** it would take them to do it manually and keep that data from ending up back online.

All clients have to do is:

- +** **Create an account** and tell us whose personal data we'll be removing. We recommend you register with the email address you use most often to help us find the most matching online records.
- ✓** **Grant us the right to work for you.** We will contact data brokers on your behalf to request your personal data removal.
- ♥** **Kick back and watch us work.** We will handle any objections from data brokers and keep you updated on our progress every step of the way.

Types of personal information data brokers usually hold



Different data brokers will collect different types of data, depending on their specialty.

The most common data broker types are:



People search sites

Create extensive profiles, including contact details, and background information, that they sell or publish online for anyone to see.



Marketing data brokers

Collect data on your online browsing habits and sell it for marketing purposes.



Recruitment data brokers

Collect data to create background reports and offer screening services to HR officers.



Risk mitigation brokers

Collect background data such as health information or police and court records and sell assessment reports to various investment companies and businesses.



Financial information brokers

Collect financial and background information and sell it to credit companies or banks.

Real-life use cases to improve personal data privacy



Data brokers **sell addresses and contact details** for anyone to buy online, exposing people to potential stalking and physical violence. This has even led to cases where domestic abuse victims were **tracked down** by their abusers yet data brokers still refused to remove their data.

[Read more](#)



Health insurance companies could actually **raise your rates** based on your online activity. These companies are teaming up with data brokers to collect data that could be used as **determinants of health**.

[Read more](#)



Some data brokers have been charged with conspiracy to commit **mail and wire fraud** for intentionally supplying data lists of **elderly and vulnerable people** to scammers.

[Read more](#)



US only. Despite guidelines indicating how people search sites should and shouldn't be used, **criminals** have been known to use the information on these sites to **target their victims**. One identity thief used the data of 51 individuals, which they acquired from a people search site, to take out thousands in **fraudulent loans**.

[Read more](#)



Huge loans have been taken under people's names without them even knowing about it. Cybercriminals from the underground cybercrime platform SSNDOB were stealing **SSNs** and other sensitive **personal information** from large data brokers like Dun & Bradstreet in order to **steal identities**.

[Read more](#)



Many data brokers sell bulk data to **companies targeting vulnerable and disadvantaged groups**. These lists have titles such as "Tough Start: Young Single Parents," "Ethnic Second-City Strugglers," or "Rural and Barely Making It." This practice exposes people to even more **discrimination**, both online and offline.

[Read more](#)



Almost everyone experiences **robocalls** from time to time. If you ever wondered how they keep getting your number, the answer is data brokers. They often **sell your phone number** to companies to form these call lists.



Data brokers often put up **addresses and contact details** for anyone to buy online, exposing people to potential stalking and **physical violence**. This can be particularly dangerous for victims of **domestic abuse** who can be easily tracked by their abusers using people search sites.

[Read more](#)



US only. People search sites publish your personal information, including details about **family members**, for anyone to look up online. It has even led to instances of **children being endangered**.

[Read more](#)





Why subscribe?

While data privacy laws and regulations protect individuals' rights to data privacy, **in theory**, it can take **more than 300 hours** for an individual to actually remove their personal information from data brokers' databases, just once.

This isn't always enough, though. In most cases, data brokers will collect your personal information again after some time, making data removal an ongoing effort.

Through our subscription-based service, we ensure your data stays off the market by conducting repeated, ongoing removals. Our yearly subscription is **especially advantageous** as it comes with an extra 50% discount and saves you years worth of manual data removal.

As part of our subscription-based service we:

-  Contact data brokers to request they remove all data associated with our customer from their databases. This may include highly sensitive data such as SSNs, login credentials, browsing and purchase histories, etc.
-  Send opt-out requests to people search sites such as BeenVerified and Intelius on behalf of our customers, removing personal details such as addresses, household members, asset information, and more from their publicly searchable databases.
-  Resend opt-out requests periodically to ensure their data does not respawn on databases we have already removed it from.
-  Continually search for and add more data brokers to our contact list, expanding the area of search for records belonging to our customer.

What makes Incogni stand out

With the online privacy arena changing, there are a few entities that offer some kind of personal data removal service. Here's what sets Incogni apart from the rest



Cover a wider market

While most personal data removal services focus on the US, Incogni covers the US, UK, EU, Switzerland, and Canada, making it a more widely accessible tool.



Work with all data broker types

Most personal data removal services focus exclusively on People Search Sites. We offer data removal from all data broker types.



Fully automated process

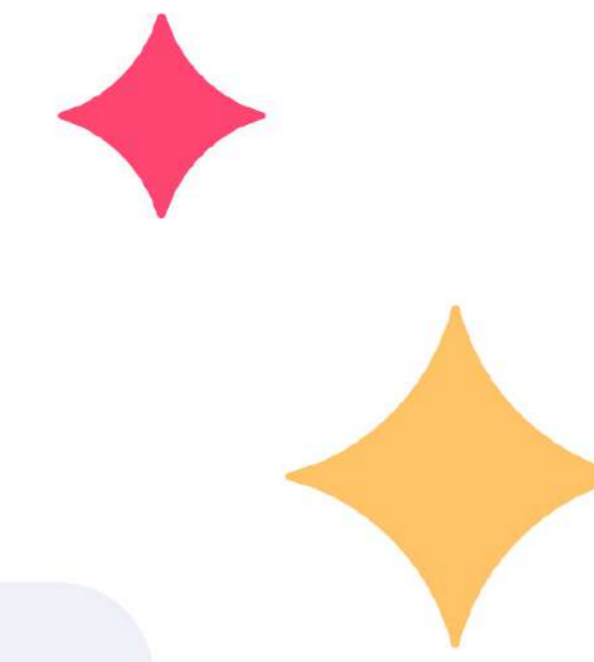
Incogni makes the data removal process super easy for users. After the initial sign-up and subscription, we handle everything else, including follow-up questions or request denials. **While some personal data removal services contact data brokers for you, they often leave you to handle all of the follow-up communication on your own, which can be deliberately confusing.**



Surfshark's experience in cybersecurity

Incogni was created by a team of Surfshark professionals who have taken their hands-on experience developing successful online security tools such as Surfshark VPN, Alert, and Search and applied it to Incogni.

FAQ



Can I have multiple emails or home addresses?

At this time, we do not have an option to add multiple emails or physical addresses to one account. We recommend using your main (the most used) email and physical address to have the highest chance that your personal data is found and removed.

How do you know if a data broker has my personal data?

We use an algorithm that predicts how likely it is that a particular data broker has your data. We can only know for certain beforehand with people search sites as we have access to their public databases.

How do you know if a data broker removed my personal data?

The data brokers confirm the records have been removed, the same way they would if you request removal yourself. If caught lying, the fines for breaking data privacy laws and regulations are significantly detrimental to the broker.

How long does it take to remove my data from data broker databases?

Some of the data brokers respond to our requests on the same day, while others really do take their time and may respond in a month. As per GDPR and CCPA, they are obliged to process the request in a 30-45 days period, so it should not take longer than that. However, data brokers may violate these terms, leading to longer response times. Additionally, data removal is an ongoing process and will be restarted regularly.

Can data brokers collect my information again after they have removed it?

Yes, many data brokers will likely acquire your personal information again. This depends on whether they use a suppression list and how often they refresh their databases. However, Incogni conducts monthly checks to ensure your data is not added again for as long as you are subscribed.