

Rabbitproof Data Processing Agreement

Version 21 October 2026. This agreement is between Rabbitproof (ABN 53 752 373 218) and each customer who uses Rabbitproof on their website. It sets out, in writing, what Rabbitproof does with information about the visitors to a customer's website. It forms part of the Terms (rabbitproof.com.au/terms) and applies to every customer, with no need to sign.

Rabbitproof is not available in the European Union, Norway, Iceland, Liechtenstein, the United Kingdom or Switzerland.

1. Who decides what

- The customer (the website owner) decides how information about the visitors to their website is used, and Rabbitproof acts for them. In privacy law the customer is called the controller of that information, and Rabbitproof the processor.
- **One exception:** when a device or network is identified as a bot on one website, Rabbitproof uses what it learned to protect every website that uses Rabbitproof (the shared list of known bots). Rabbitproof decides that use itself, for security, and is responsible for it. That information is used for that security purpose only.
- Information about the customer's own account (email, billing, support) is Rabbitproof's own, under the Privacy Policy (rabbitproof.com.au/privacy), not this agreement.

2. What is processed

What information is processed, whose, and for how long, is set out in Annex I. Rabbitproof processes it only to tell people from bots on the customer's website and to block bots, and for nothing else: no advertising, no analytics sold, no profiles.

3. Rabbitproof's commitments

1. Rabbitproof processes the information only as the customer instructs: this agreement, the service's settings, and what the customer chooses in the dashboard or the WordPress plugin (for example the places Geoblock blocks).
2. Everyone at Rabbitproof with access to it is bound to keep it confidential.
3. Rabbitproof keeps the security measures in Annex II.
4. Rabbitproof uses only the companies on its published list (rabbitproof.com.au/compliance), under terms at least as protective as these. It tells customers by email 30 days before a new one is added, and updates the list. A customer who objects can stop the product or delete their account before the change takes effect; no part of a billing period is refunded, as in the Terms.
5. Rabbitproof helps the customer answer requests from their visitors (to see, delete or stop the use of their information). Rabbitproof keeps visitors' internet addresses only in a coded form, so it can find a visitor's records only from the internet address the visitor used, or the reference shown on the page that refused them.
6. Rabbitproof tells the customer of a breach of security affecting information about their visitors without undue delay, and within 48 hours of becoming aware of it.
7. At the end of the service, see Annex I, "When the service ends".

8. Rabbitproof makes available what the customer needs to check these commitments: it answers one written security questionnaire a year at no charge; any further audit is at the customer's cost, with 30 days' notice, at most once a year.

4. The customer's commitments

- The customer is allowed, under the law that applies to them, to use Rabbitproof on their website to protect it from bots.
- The customer tells their visitors, in their own privacy policy, that the website uses Rabbitproof, including its cookie and the check in the browser. A paragraph to copy is on rabbitproof.com.au/compliance: "This website uses Rabbitproof (rabbitproof.com.au) to protect it from bots and spam. When you visit, Rabbitproof checks your browser and device and the internet address you connect from, to tell people and bots apart. It sets a cookie so you are not checked again on every page. This information is used only to protect this website and other websites that use Rabbitproof, and is kept for a short time. Rabbitproof's privacy policy: rabbitproof.com.au/privacy."
- The customer decides whether their visitors need to agree to the check under the rules of their own country.
- The customer does not use Rabbitproof for a business based in, or a website aimed at people in, the places listed at the top of this agreement.

5. Where it is handled

Rabbitproof is based in Australia. The service runs on Cloudflare's network, which has data centres around the world, so information may be handled and stored outside the customer's country. Rabbitproof's network check runs on its own server in Sydney, Australia.

6. Liability, term and law

- Liability is the same as in the Terms, as far as the law allows: Rabbitproof is not responsible for indirect losses, and its total responsibility is limited to the fees paid in the last 12 months.
- This agreement lasts as long as the customer uses Rabbitproof, and after that for as long as Rabbitproof still holds information about their visitors (Annex I).
- This agreement is governed by the same law as the Terms (Australian law).
- If this agreement and the Terms disagree on how information about visitors is handled, this agreement wins.
- Questions: support@rabbitproof.com.au.

Annex I: the processing

Whose information: the people who visit the customer's website.

What information:

- Their internet address. Kept only in a coded form (a keyed code), never the address itself, except in Rabbitproof's network check server's log, which keeps the address for 7 days.
- The country and network the address belongs to.
- Technical details from the browser and device (such as the screen, graphics, time zone, language and browser), and a device code worked out from them. Each website's records keep the code, not the

details, except the name of the graphics chip for up to 2 hours. The shared list of known bots keeps only the graphics chip family (for example "NVIDIA RTX"). Rabbitproof's record of each decision keeps the details themselves (below).

- The page address (for a form, also the names of any query parameters, never their values), the referring website, and the kind of browser. Never anything typed into a form.
- The internet address the device's network check connection came from, in a coded form.
- On Bot Management with Geoblock on: the connection's country and the device's time zone, compared with the places the customer chose to block. A time zone that belongs to no country (such as UTC) does not block.

How long it is kept:

Record	Kept for
The website's list of requests	7 days, at most 5,000
Visitors blocked	24 hours
Visitors the customer unblocked	7 days
Daily counts behind the dashboard's numbers	32 days
Forms sent to the website	30 days
Request counts for billing (no information about visitors)	100 days
Short working records for the checks	10 minutes to 24 hours
Rabbitproof's record of each decision	About 3 months
Devices identified as bots (the shared list)	90 days after they were last seen
Rabbitproof's network check server's log	7 days

Rabbitproof's record of each decision holds, for each checked request, the decision and its reasons, the internet address in a coded form, the page address, the referring website, the kind of browser, country and network, and on a check from a browser also the device details listed above. It is kept to look into wrong refusals.

When the service ends: the account and its websites are deleted at once, and so are the records about the visitors to its websites. A request already on its way when a website is deleted may add a few records in the next minute; those run out on the schedule above.

Annex II: security measures

- Visitors' internet addresses are kept only in a coded form, under a separate key for each website, except in the network check server's 7-day log.
- Customer passwords are stored only as a slow, salted and peppered hash; sign-in and email links and secret keys only as keyed codes; two-step sign-in secrets and website secret keys only in encrypted form. The count of wrong passwords is kept against a code of the email address, never the address itself.
- Rabbitproof's admin area is behind Cloudflare's access control and two-step sign-in, with short admin sessions (8 hours at most, 1 hour unused) and a log of admin actions kept for a year.

- Customer sign-ins end after 30 days, after 7 days unused, on a password change, and on "sign out everywhere". Expired sign-ins, links and limits are deleted every hour.
- Limits on sign-in, sign-up, website verification and every email sent.
- The network check server: key-only access, password sign-in turned off, and a service account used for nothing else.