Privacy Policy — Public Coverage Checker & Map the Gap

Effective date: August 2026 Last updated: August 2026

Welcome to Streetwave's public coverage tools, operated by Streetwave Ltd ("Streetwave", "we", "us" or "our").

This privacy policy covers our **Public Coverage Checker** and **Map the Gap**, our signal-problem reporting tool (together, the "Service"), available at https://app.streetwave.co — including the council-branded versions of those tools that are linked from, or embedded on, partner council websites.

Streetwave respects your privacy and is committed to protecting your personal data. This policy explains what we collect when you use the Service, why we collect it, who we share it with, and the rights you have. Please use the Glossary in section 16 to understand the meaning of any terms used in this policy.

> **This policy at a glance**
>
> - **We don't ask who you are.** The Service has no accounts or logins, and the Map the Gap report form does not collect your name or contact details.
> - **What a report contains:** a location, whether you were indoors/outdoors/in a car, the network you were using, whether you'd switch network, what went wrong and how often, your connection to the area (resident / business / visitor), how the problem affects you, and the date and time you submit it. That's it.
> - **Why we collect it:** so the relevant mobile operator and, where applicable, the local council for that area have real-world evidence of where mobile coverage needs to improve.
> - **Who sees it:** the relevant mobile operator (and, for virtual networks, the host network) and the relevant partner council — plus the service providers that run our infrastructure (section 9). Anything we publish more widely is anonymised and aggregated.
> - **Cookies:** we do not set cookies. The map is drawn using a third-party map service (section 2.6), and Google reCAPTCHA protects the report form against spam and abuse (section 6).

---

1. About this policy and who we are

1.1 Purpose of this policy

This policy tells you how we collect and process personal data through your use of the Service — whether you are checking measured mobile coverage for a location, or reporting a signal problem through Map the Gap.

The Service is **not** intended for children under the age of 16 and we do not knowingly collect personal data relating to children. If you are under 16, please do not submit a Map the Gap report or provide us with any personal data.

You should read this policy together with any other privacy notice we may provide on specific occasions when we are collecting or processing personal data about you. This policy applies to the Service only; our corporate website and our commercial products and services for organisations are covered by our main website privacy policy.

1.2 Who we are (the controller)

Streetwave Ltd is the controller responsible for the personal data processed through the Service as described in this policy.

- **Legal entity:** Streetwave Ltd (registered in England & Wales)
- **Registered office:** Wesley Clover Innovation Centre, Coldra Woods, Chepstow Road, Newport, Wales, NP18 2YB

We have not appointed a Data Protection Officer because we are not required to do so under UK data protection law. Privacy queries should be directed to the contact details below.

"In partnership with" your council. The Service is commissioned by, and run in partnership with, local authorities ("partner councils"), and the version of the Service you use may carry the name and logo of the partner council for your area. The Service itself is operated by Streetwave, and Streetwave is the controller for the data you submit through it. When we pass a Map the Gap report (or aggregated coverage insight) to a partner council, that council becomes a separate, independent controller of the information it receives and its own privacy notice applies to what it does next — see sections 2.4 and 9. Our agreements with partner councils record our respective data protection responsibilities.

1.3 Contact details

If you have any questions about this privacy policy, want a report taken down, want to exercise any of your rights, or have a privacy concern, please contact us:

- **Privacy contact:** George Gibson
- **Email:** info@streetwave.co
- **Post:** Streetwave Ltd (Privacy), Wesley Clover Innovation Centre, Coldra Woods, Chepstow Road, Newport, Wales, NP18 2YB
- ICO Reference: ZC131077

You have the right to complain to the Information Commissioner's Office (ICO), the UK regulator for data protection issues (www.ico.org.uk or telephone 0303 123 1113). We would, however, appreciate the chance to resolve your concerns before you approach the ICO — see section 14 on our complaints procedure.

1.4 Changes to this privacy policy

We keep this privacy policy under regular review. This version is dated at the top of this document. We will update the date when we make any material changes. Historic versions are available on request.

1.5 Third-party links

The Service and the pages around it may contain links to third-party websites — including partner council websites, mobile network operators' websites, and Ofcom resources. When you follow a link off the Service,

you leave our service. We do not control those third-party sites and are not responsible for their privacy practices. We encourage you to read the privacy policy of every website you visit.

---

2. How the Service works — and who processes your data

We want to be transparent about the data flow behind the Service, because several organisations are involved in improving mobile coverage.

2.1 What the Service is

The Public Coverage Checker lets you look up independently measured, real-world mobile network performance for locations in participating council areas, so you can see which networks actually work where you live, work or travel. The coverage results you see are generated from Streetwave's own network surveying (for example, measurement equipment carried on council vehicles). That measurement data is about networks and places, not about you, and is not your personal data.

Map the Gap lets you report a real-world signal problem — a dropped call, slow data, or no signal at all — by putting it on the map. Your report becomes part of an evidence base that the relevant mobile operator and, where applicable, the local council use to understand exactly where investment in mobile coverage is needed.

By design, the Service collects as little identifiable personal data as possible. There are no user accounts or logins, no payments, and the Map the Gap report form does not ask for — and does not collect — your name or contact details.

2.2 Our own backend (AWS UK)

All of the data collected through the Service — coverage-checker lookups and Map the Gap reports — is stored on our own backend, hosted in the **United Kingdom region of Amazon Web Services (AWS)**. AWS acts as our hosting provider (a data processor) and does not use this data for its own purposes.

2.3 Rybbit (privacy-first analytics)

We use **Rybbit** as our web analytics platform. Rybbit is a cookieless, privacy-friendly analytics tool hosted in the European Union (Hetzner, Germany). Rybbit does not set cookies on your device, does not use cross-site tracking, does not create persistent identifiers, and does not store raw IP addresses. Data is aggregated for site-traffic analysis only. Where Rybbit processes personal data on our behalf, it does so as our **data processor** under its Data Processing Agreement. For more information see rybbit.com/privacy and rybbit.com/dpa.

2.4 Partner councils and mobile network operators (recipients of reports)

When you submit a Map the Gap report, we share it with:

- **the relevant mobile network operator** — the network you told us you were using and, where that network is a virtual operator (an MVNO), the host network whose masts and infrastructure it runs on, since that is who can act on coverage problems; and

- **where applicable, the partner council** for the area the report relates to,

so they know exactly where to invest. Each of them is a separate, **independent controller** of the report data it receives from us, and processes it under its own privacy notice and its own lawful basis (for a council, typically its public task of promoting connectivity and economic wellbeing in its area). Reports we share do not contain your name or contact details, because we do not collect them.

2.5 Google reCAPTCHA (form security)

The Map the Gap report form is protected by **Google reCAPTCHA**, a service provided by Google (Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland, and Google LLC in the United States), which helps us distinguish real reports from automated spam and abuse. Because councils and operators rely on this data as evidence, keeping fake and bulk submissions out of the dataset is essential to the integrity of the Service.

reCAPTCHA works by collecting and analysing information about your device and your interaction with the form — which may include your IP address, browser and device characteristics, and how you interact with the page — and sending it to Google for risk analysis. Google processes this information in accordance with the Google Privacy Policy (https://policies.google.com/privacy) and Terms of Service (https://policies.google.com/terms). See section 6 for what this means for cookies, and section 10 for international transfers.

2.6 Map tiles and address search

The interactive map in the Service is drawn using map tiles from OpenFreeMap, a third-party map service which uses data provided by OpenStreetMap.

Address search and geocoding is provided by Ideal Postcodes (https://ideal-postcodes.co.uk/).

When the map loads, your browser requests the tiles for the area you are viewing directly from the map service's servers, which therefore receive your IP address and the general area you are looking at. The map service does **not** receive your report: any pin you drop, and everything you enter in the report form, goes only to our own backend (section 2.2). Similarly, when you type into the address search box, the text you type is sent to the address-lookup service in order to return matching places.

We deliberately use privacy-respecting, non-advertising map services: they do not set cookies on the Service, and we do not share your report data with them. OpenFreeMap states in its own privacy policy that it does not use cookies or tracking technologies and does not log IP addresses in normal operation, and Ideal Postcodes is a UK-based provider which does not use address queries to identify individual users.

---

3. The data we collect about you

Personal data means any information about an individual from which that person can be identified. It does not include data where the identity has been permanently removed (anonymous data).

We designed the Service to collect the minimum information needed for coverage evidence, and we do not link it to your identity. However, we take a cautious approach: a precise location (for example, a dropped pin at

your home, or an address you search for) can, in combination with other information, relate to you or your household — so we treat the data below as personal data and protect it accordingly.

We may collect, use, store and transfer the following categories of data about you:

- **Location Data:** the location you report or look up — an address or place you type into the search box, the coordinates of a pin you drop on the map, or, if you choose to use the "find my location" control, the coordinates reported by your device (shared only with your permission via your browser's location prompt; we never access your device's location otherwise) — and, for Map the Gap reports, whether you were indoors, outdoors or in a car at the time.
- **Network Data:** the mobile network you tell us you were using, and whether you would switch network purely for better performance.
- **Service-Quality Data:** what went wrong (for example, no signal at all, slow data, dropped calls, poor call quality, can't send messages, or something else), how often it happens, and the date and time the report is submitted.
- **Context Data:** your connection to the area (resident, business and/or visitor) and the broad categories of life the problem affects (work/business, health, education, daily life, "just frustrating", and/or safety concern). These are high-level tick-box categories that help councils and operators prioritise — see section 3.2 on why you should not add sensitive detail.
- **Lookup Data:** the locations you search in the Public Coverage Checker and the results shown, which we store only in anonymised / aggregate form with no user identifier.
- **Correspondence Data:** if you contact us (for example, to ask a question or request that a report is taken down), the contact details you use and the content of your message.
- **Security Data:** information collected by Google reCAPTCHA to verify that a report is submitted by a human (see sections 2.5 and 6).
- **Technical Data:** limited technical information about your visit collected by Rybbit — such as approximate country/region (derived from your IP address at the time of the request, then discarded), browser type, device type, operating system, referring URL and pages viewed. This data is not linked to you as an individual.
- **Server Log Data:** like almost every online service, our web servers keep short-lived technical request logs (including IP address, request time and URL requested) for security, abuse-prevention and troubleshooting purposes. These logs are kept separate from reports and lookups, and we do not use them to identify who submitted a report.
- **Usage Data:** aggregated information about how visitors use the Service (for example, which areas are looked up most often).

We also use **Aggregated Data** (statistical or demographic summaries, and anonymised coverage-evidence datasets) for the operation of the Service and our business. This may be derived from the data above but is not treated as personal data because it does not directly or indirectly identify you.

We do not:

- collect your name or contact details through the Coverage Checker or the Map the Gap report form
- operate user accounts or logins
- process any payments through the Service
- collect Financial Data (bank or card details)

- knowingly collect Special Category Data (see section 3.2)
- collect data about criminal convictions or offences
- use your data to sell you anything, or share it with anyone for marketing purposes

3.1 If you don't give us your data

The Coverage Checker works without you providing any identifiable personal data, and Map the Gap reports are submitted without your name or contact details. You only share identifying personal data with us if you choose to contact us directly (for example by email).

3.2 Please do not submit Special Category Data

The Map the Gap form is deliberately built around tick-box options rather than free text. The "How does it affect you?" categories (including "Health" and "Safety Concern") are broad, high-level indicators used only to help councils and operators understand and prioritise the real-world impact of poor coverage. They are not intended to — and, submitted as designed, do not — reveal anything specific about you, and reports are not linked to your identity.

The only place you can type freely is the address search box — please only ever enter the address or place you want to find. **If the form offers you a text box anywhere (for example, if you pick "Something else" and are invited to describe it), or if you contact us by email, please do not include personal details — yours or anyone else's — or any Special Category Data.** Special Category Data includes information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic or biometric data, and data concerning health, sex life, or sexual orientation — and, in the UK, information about criminal convictions or offences. For example, please do not write things like "I couldn't call my therapist" or "I missed a hospital appointment"; "no signal at all" and "health" tell the council everything it needs to know.

If you believe a submission contains sensitive information about you or another person, please contact us (section 1.3) and we will remove or anonymise it without undue delay. We reserve the right to remove, anonymise or delete any submission that in our reasonable view contains Special Category Data, personal details, or content that is unlawful, abusive or unrelated to mobile coverage.

---

4. How your data is collected

We collect data through:

- **Direct interactions.** You give us Location, Network, Service-Quality and Context Data when you submit a Map the Gap report, and Location/Lookup Data when you use the Public Coverage Checker. You give us Correspondence Data if you email us or otherwise contact us.
- **Automated technologies.** As you use the Service, we collect limited, non-identifying Technical Data and Usage Data via Rybbit analytics (see section 2.3), and our servers generate short-lived Server Log Data (see section 3). When you submit a report, Google reCAPTCHA collects Security Data as described in section 2.5, and using the map or address search involves the third-party map services described in section 2.6.

- **Partner councils and operators.** We do not receive personal data about you from partner councils or mobile network operators in connection with the Service.

---

5. What happens to your report

So there are no surprises, here is the life cycle of a Map the Gap report:

1. **You submit the report** — location, setting, network, willingness to switch, issue(s), frequency, your connection to the area, impact categories, and the date and time of submission. No name, no contact details.
2. **We store it** on our AWS UK backend as part of the coverage-evidence dataset for the relevant area.
3. **We share it** with the relevant mobile network operator and, where applicable, the partner council for the area, as described in section 2.4 — so they know exactly where coverage is failing people and where to invest.
4. **We aggregate it.** Reports feed anonymised, aggregated statistics and insights (for example, "142 reports of no signal in this ward in the last quarter, 68% from residents, most citing daily life and work impacts") that we may publish, include in our products and reporting for councils, operators and other public-sector bodies, or use to improve the Service. Individual reports are not published.
5. **It stays useful.** Because network investment decisions can take years, the underlying evidence base is retained as described in section 12.

---

6. Cookies and similar technologies

We do not set cookies on your device when you use the Service, and we have deliberately chosen a first-party, privacy-friendly architecture:

- **Rybbit analytics is cookieless and storage-less** — it does not set cookies, does not use localStorage or sessionStorage, and does not create persistent identifiers (see section 2.3).
- **We do not run Google Analytics, Google Ads tags, Meta Pixel, TikTok pixel or any similar third-party marketing or advertising tags** on the Service.
- **We do not use advertising cookies, re-targeting cookies, cross-site tracking cookies, or affiliate tracking cookies** on the Service.
- **We do not embed social-media widgets, advertising tags, tracking pixels or third-party fonts.** The only third-party components in the Service are the map services (section 2.6), which do not set cookies, and Google reCAPTCHA (below) — and neither is used for advertising or marketing.

The one exception is Google reCAPTCHA on the Map the Gap report form. To tell humans and bots apart, reCAPTCHA may read and set cookies on Google domains and collect information about your device and how you interact with the form (see section 2.5). We use reCAPTCHA solely for the security and integrity of the Service — to prevent spam, fraudulent and automated submissions from polluting an evidence base that councils and operators rely on — and not for advertising or marketing. Google's use of this information is governed by the Google Privacy Policy (https://policies.google.com/privacy) and Terms of Service (https://policies.google.com/terms).

We consider this use of reCAPTCHA to be strictly necessary to provide the reporting service you have asked for and to protect the security and integrity of the Service, consistent with the Privacy and Electronic Communications Regulations 2003 (as amended, including by the Data (Use and Access) Act 2025) — which is why the Service does not display a cookie-consent banner. If our use of these technologies changes, section 6.2 applies.

6.1 Browser-level controls

You can limit tracking across the web by setting your browser to block third-party cookies, using private/incognito mode, using the tracking-protection features built into Safari, Firefox, Brave and other browsers, or using the Global Privacy Control (GPC) signal where your browser supports it. These are browser-level settings and apply to all websites you visit, not just the Service. Blocking Google cookies may affect your ability to pass the reCAPTCHA check when submitting a report.

6.2 If this changes in the future

If we ever add any further cookie, local-storage entry, or similar technology to the Service — whether strictly necessary (e.g. security) or non-essential (e.g. analytics, advertising, embedded media) — we will update this policy and, where consent is required by PECR (as amended by the Data (Use and Access) Act 2025), put in place a compliant consent mechanism before the change goes live.

---

7. How we use your data, and our lawful bases

We will only use your personal data when the law allows us to. Most commonly, we will rely on **legitimate interests** — the Service is a free, anonymous-by-design public tool, and we do not use your data for marketing. See the Glossary in section 16 for more detail on each lawful basis.

7.1 Purposes for which we use your data

Purpose / Activity	Type of data	Lawful basis
To run the Public Coverage Checker and show you measured network performance for the locations you look up	(a) Location (b) Lookup	Legitimate interests (to provide the free lookup service you have asked for and to help the public make informed decisions about mobile networks)
To accept and store Map the Gap reports as part of the coverage-evidence dataset	(a) Location (b) Network (c) Service-Quality (d) Context	Legitimate interests (to operate a public-benefit community tool that identifies real-world mobile coverage problems)
To share Map the Gap reports with the relevant mobile network operator and, where applicable, the relevant partner council	(a) Location (b) Network (c) Service-Quality (d) Context	Legitimate interests (to give operators and councils the location-specific evidence they need to target investment in mobile coverage — the purpose for which you submitted the report)

Purpose / Activity	Type of data	Lawful basis
To produce, publish and commercially supply anonymised, aggregated coverage statistics and insights (which are not personal data once aggregated)	(a) Location (b) Network (c) Service-Quality (d) Context (e) Lookup (f) Usage	Legitimate interests (to build and supply independent evidence on UK mobile coverage and run our business)
To review, moderate, remove or anonymise submissions (including any containing Special Category Data or personal details)	(a) All report data (b) Correspondence	Legitimate interests (to keep the dataset accurate and lawful, and to ensure we do not retain Special Category Data)
To protect the Service against spam, abuse and fraudulent submissions (including via Google reCAPTCHA)	(a) Security (b) Technical	Legitimate interests (to maintain the security and integrity of the Service and the reliability of the evidence base)
To understand how visitors use the Service in aggregate (analytics via Rybbit)	(a) Technical (b) Usage	Legitimate interests (to improve the Service, our content and our products)
To respond to an enquiry, takedown request, rights request or feedback you send us	(a) Correspondence	(a) Legitimate interests (to respond to queries and operate the Service responsibly) (b) Legal obligation (where you exercise a legal right)
To manage our relationship with partner councils, including reporting on the operation of the Service	Aggregated Data (not personal data)	Legitimate interests (to perform our contracts with partner councils)
To comply with legal, regulatory or tax obligations	(a) Correspondence (b) any data subject to a legal demand	Legal obligation

We may process your personal data on more than one lawful basis depending on the specific purpose. Please contact us if you need details about the specific legal basis we are relying on.

7.2 No marketing

We do not collect your contact details through the Service, and we will not use anything you submit through the Service to send you marketing. If you contact us by email, we will use your details only to deal with your enquiry.

7.3 Change of purpose

We will only use your personal data for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason that is compatible with the original purpose. If we need to use your

personal data for an unrelated purpose, we will update this policy and, where required, notify you and explain the legal basis which allows us to do so.

---

8. Automated decision-making and profiling

We do **not** make decisions about you using purely automated means that produce legal or similarly significant effects for you (the kind of processing restricted by the UK GDPR's automated decision-making provisions, as amended by the Data (Use and Access) Act 2025), and we do not profile you.

For transparency:

- **The Coverage Checker** displays independently measured network performance for the location you look up. Results depend on the location and our measurement data — not on who you are. We do not use your data to change what different visitors see.
- **Google reCAPTCHA** uses automated risk analysis to distinguish humans from bots when a report is submitted. This is a security measure; it does not produce legal or similarly significant effects for you. If a submission is blocked in error, you can contact us (section 1.3) and we will review it manually.

If we ever introduce automated decision-making that produces legal or similarly significant effects, we will update this policy in advance, explain the logic involved and the significance and envisaged consequences for you, and tell you how to request human intervention, express your point of view, or contest the decision.

---

9. Who we share your data with

We may share data collected through the Service with the following categories of recipient, strictly for the purposes described in this policy:

- **Mobile network operators** — the operator identified in your report (and, where that network is a virtual operator, the host network whose infrastructure it uses) receives the report so it can investigate and target investment. Each operator is an **independent controller** of the report data it receives and processes it under its own privacy notice.
- **Partner councils** — where the report relates to a participating council area, the relevant council receives the report (and aggregated insights) as evidence for improving local connectivity. Each council is an **independent controller** of what it receives, typically processing it under its public task. Please note that information held by a council may be subject to the Freedom of Information Act 2000 and the Environmental Information Regulations 2004; reports contain no names or contact details, and we would expect precise locations to be handled by councils in line with their own disclosure policies.
- **Amazon Web Services (AWS)** — hosting provider for our backend, UK region (data processor).
- **Rybbit** — our analytics provider, EU-hosted (data processor).
- **Google** — provider of reCAPTCHA form security (see sections 2.5 and 6). Google processes reCAPTCHA data in accordance with its own privacy policy and terms.
- **Map service providers** — the third-party map-tile and address-search services described in section 2.6 receive the technical requests needed to draw the map and find places. They do not receive your submitted reports.

- **Our service providers** — reputable third-party platforms we use to run our business (for example, email and IT systems used to handle correspondence). They act as our data processors under written agreements and may only process personal data on our instructions.
- **Professional advisers** — including lawyers, accountants, auditors, and insurers, where reasonably necessary.
- **Regulators and other authorities** — including the ICO, HM Revenue & Customs, law enforcement and courts, where we are required to by law.
- **Other third parties** — in the event of a sale, restructure or merger of our business, in which case we may share data with the prospective buyer or new owner under strict confidentiality obligations. Anonymised, aggregated coverage datasets (which are not personal data) form part of Streetwave's assets and may be supplied to councils, operators, government bodies and other customers as part of our business.

We require all our data processors to respect the security of your personal data and to treat it in accordance with the law. We do not allow our service providers to use your personal data for their own purposes.

We do not sell personal data, and we do not share personal data with any third party for marketing purposes.

---

10. International transfers

Where possible, your data stays within the UK or EEA:

- **Streetwave's own backend** (all Coverage Checker and Map the Gap data): hosted on **AWS in the United Kingdom region**. No Streetwave-backend data is transferred outside the UK in the ordinary course of operation.
- **Rybbit analytics:** processed in the EU (Germany) — the UK Government has confirmed that the EEA provides an adequate level of protection for personal data, so no additional safeguards are required.
- **Map services (section 2.6):** postcode lookup and geocoding is processed and controlled by a data controller in London, UK. Map tiles are served by OpenFreeMap, which states that it does not log IP addresses in normal operation; tile delivery may pass through a global content-delivery network so that maps load quickly.
- **Google reCAPTCHA:** Google may process Security Data on servers outside the UK and EEA, including in the United States. Where this happens, the transfer is protected by one or more of the safeguards required by UK data protection law — the UK–US Data Bridge (the UK Extension to the EU–US Data Privacy Framework, where the Google entity is certified), the UK International Data Transfer Agreement or Addendum to the EU Standard Contractual Clauses, or another lawful transfer mechanism.
- **Correspondence:** if you contact us, your enquiry may be handled through business systems (such as our email and CRM platforms) whose providers are located in, or support their services from, the United States. Where this involves a transfer of personal data outside the UK and EEA, we ensure it is covered by one of the safeguards listed above.

Where any of our third-party processors transfer personal data outside the UK and EEA, we ensure that an appropriate safeguard is in place before the transfer occurs. You can request further details by contacting us using the details in section 1.3.

---

11. Data security

We have put in place appropriate technical and organisational security measures to prevent your personal data from being accidentally lost, used, accessed, altered or disclosed in an unauthorised way. These include access controls, encryption in transit (HTTPS/TLS), limiting access to personal data to employees, agents, contractors and third parties who have a business need to know, and requiring them to process personal data only on our instructions and subject to a duty of confidentiality.

We have procedures in place to deal with any suspected personal data breach and will notify you and any applicable regulator (including the ICO) of a breach where we are legally required to do so.

---

12. Data retention

We will only retain personal data for as long as reasonably necessary to fulfil the purposes we collected it for, including to satisfy any legal, regulatory, tax, accounting or reporting requirements. To determine the appropriate retention period, we consider the amount, nature and sensitivity of the data, the potential risk of harm from unauthorised use or disclosure, the purposes for which we process it, and whether we can achieve those purposes through other means.

A note on why coverage data is kept long-term: the point of the Service is to evidence where investment is needed, and network investment cycles run over years, not weeks. Reports are therefore retained — without any user identifier — as part of the long-term coverage-evidence dataset.

Our standard retention periods are:

Data	Retention
Map the Gap reports (location, setting, network, switching preference, issue, frequency, connection to area, impact categories, date/time of submission)	Stored without any name, contact details or user identifier. Retained as part of the coverage-evidence dataset for as long as it remains useful evidence for network investment, subject to periodic review — and we may reduce the precision of stored locations once a report has served its immediate purpose. Any Special Category Data or personal details we become aware of (whether identified by us or reported to us) are deleted or anonymised without undue delay
Coverage Checker lookups	Stored in anonymised / aggregate form — no user identifier is kept alongside the location. Retained indefinitely as part of the aggregate usage dataset
Rybbit analytics data	Up to 5 years, then automatically deleted
Google reCAPTCHA data	Held by Google under its own privacy policy and retention schedule
Server request logs (IP address, request time, URL)	Up to 30 days, then automatically deleted. Not linked to reports or lookups

Data	Retention
Correspondence (enquiries, takedown requests, feedback)	24 months after the last interaction, unless a longer period is required for legal reasons
Records of complaints and Subject Access Requests	3 years after the matter is closed
Records we are legally required to keep for tax and accounting purposes	6 years from the end of the relevant financial year (Companies Act 2006 and HMRC rules)

In some circumstances we may anonymise personal data (so that it can no longer be associated with anyone) for research or statistical purposes, in which case we may use this information indefinitely without further notice to you.

---

13. Your legal rights

Under UK data protection law, you have the following rights in relation to your personal data:

- **Right of access** — to request a copy of the personal data we hold about you (a "subject access request").
- **Right of rectification** — to ask us to correct any inaccurate or incomplete data.
- **Right of erasure** ("right to be forgotten") — to ask us to delete personal data where there is no good reason for us to keep processing it.
- **Right to object** — to object to processing based on our legitimate interests on grounds relating to your particular situation. We must stop unless we can demonstrate compelling legitimate grounds that override your interests, rights and freedoms, or the processing is needed to establish, exercise or defend legal claims.
- **Right to restriction** — to ask us to suspend processing in certain circumstances, including while we verify accuracy.
- **Right to data portability** — to receive your personal data in a structured, commonly used, machine-readable format (applies only where we process data on the basis of consent or contract, and by automated means).
- **Right to withdraw consent** — where we rely on consent (we do not currently rely on consent for any processing under this policy), you can withdraw it at any time.
- **Rights in relation to automated decision-making** — as set out in section 8, we do not carry out this kind of processing.

No fee is usually required — you will not have to pay a fee to exercise your rights. However, we may charge a reasonable fee, or refuse to comply, if your request is clearly unfounded, repetitive or excessive.

What we may need from you — we may need to request specific information from you to help us confirm your identity before fulfilling a request. This is a security measure to ensure personal data is not disclosed to a person who has no right to receive it.

Time limit to respond — we try to respond to all legitimate requests within one calendar month. Occasionally it could take us longer if your request is particularly complex or you have made a number of requests; in that case we will notify you and keep you updated.

13.1 An important note about anonymity (Article 11 UK GDPR)

Because Map the Gap reports and Coverage Checker lookups are stored **without** your name, contact details or any user identifier — and we do not link them to server logs — we are usually **not able to identify which reports or lookups (if any) came from you**. Under Article 11 UK GDPR, where we cannot identify you in our data, the rights of access, rectification, erasure, restriction and portability do not apply to that data — unless you can provide additional information that enables us to identify your specific submissions. We are not obliged to collect or keep extra information about you just to be able to link data to you, and doing so would defeat the privacy-protective design of the Service.

13.2 Taking down or amending a Map the Gap report

Even where we cannot verify that a report was yours, we will still act in good faith on any reasonable request. If you want a report removed, anonymised or corrected — for example, because the pinned location is your home and you have changed your mind about reporting it — email us at info@streetwave.co with enough detail for us to find it (the location, the network, and the rough date and time of submission). We will remove or anonymise the report without undue delay.

---

14. Complaints

If you are unhappy with how we have handled your personal data, please tell us first so we have the opportunity to put things right.

14.1 How to complain to us

- **Email:** info@streetwave.co (please put "Privacy Complaint" in the subject line)
- **Post:** Streetwave Ltd (Privacy Complaint), Wesley Clover Innovation Centre, Coldra Woods, Chepstow Road, Newport, Wales, NP18 2YB

We handle data protection complaints in line with the complaints duty introduced by the **Data (Use and Access) Act 2025** (in force from 19 June 2026). In particular we will:

1. **Acknowledge your complaint within 30 days** of receipt, confirming we have it and how we will respond.
2. Take appropriate steps to investigate the issue fairly, and proportionately to its nature and complexity.
3. Keep you informed of progress and respond to you substantively **without undue delay** — within one month wherever possible. If your complaint is particularly complex, we may need longer, and we will tell you if so.

14.2 Complaining to the ICO

You also have the right to complain to the Information Commissioner's Office (ICO), the UK regulator for data protection:

- **Website:** www.ico.org.uk/make-a-complaint
- **Helpline:** 0303 123 1113
- **Post:** Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

The ICO generally expects you to have raised your complaint with the controller (us) first, and following the Data (Use and Access) Act 2025 we are required to have a process for resolving complaints — so we would always appreciate the chance to respond before you approach the ICO. Nothing in this policy affects your statutory right to complain to the ICO.

---

15. Partner councils: a note for the curious

Some users ask what their council can and cannot see. To be clear:

- Your council receives Map the Gap reports for its area (location, setting, network, switching preference, issue, frequency, connection to the area, impact categories, and the date and time) and aggregated statistics. It does **not** receive your name or contact details (we never collect them), your IP address, or any device or user identifier.
- Your council does **not** get access to individual Coverage Checker lookups; councils see aggregate usage statistics only.
- What a council does with the reports it receives — including how long it keeps them and whether it shares them (for example, with Ofcom, the UK Government or a mobile operator as part of an investment case) — is governed by that council's own privacy notice.

---

16. Glossary

16.1 Lawful bases

- **Legitimate interest** means the interest of our business in conducting and managing our business, and in operating public-benefit services, so we can provide the best and most secure experience. We make sure we consider and balance any potential impact on you (both positive and negative) and your rights before we process your personal data for our legitimate interests. We do not use your personal data for activities where our interests are overridden by the impact on you. You can obtain further information about how we assess our legitimate interests for specific activities by contacting us.
- **Consent** means processing your personal data where you have given a clear, specific, freely given and informed indication that you agree to the processing. You can withdraw consent at any time.
- **Performance of contract** means processing your data where it is necessary for the performance of a contract to which you are a party, or to take steps at your request before entering into such a contract.
- **Legal obligation** means processing your personal data where it is necessary for compliance with a legal or regulatory obligation that we are subject to.

16.2 Key parties

- **Controller** — the organisation that determines the purposes and means of processing personal data. Streetwave Ltd is the controller for the Service.
- **Processor** — an organisation that processes personal data on behalf of a controller, under a contract and only on the controller's instructions. AWS and Rybbit act as our processors.
- **Independent controller** — an organisation that determines its own purposes and means of processing data it receives. Partner councils and mobile network operators are independent controllers of the reports we share with them, and Google is responsible under its own policies for its processing of reCAPTCHA data.
- **Partner council** — a local authority that has commissioned coverage measurement and/or the Service for its area, identified on the version of the Service you use.
- **Mobile network operator** — a provider of mobile services in the UK (for example EE, Vodafone, O2, Three, or a virtual operator using their networks).

16.3 Key laws referenced

- **UK GDPR** — the UK General Data Protection Regulation.
- **Data Protection Act 2018** — the UK law that sits alongside the UK GDPR.
- **Data (Use and Access) Act 2025 (DUAA)** — the 2025 Act that amended the UK GDPR, Data Protection Act 2018 and PECR, with most provisions in force from early 2026 and the data protection complaints process in force from 19 June 2026.
- **PECR** — the Privacy and Electronic Communications Regulations 2003, which govern electronic marketing, cookies and similar technologies.
- **Freedom of Information Act 2000 / Environmental Information Regulations 2004** — the UK access-to-information regimes that apply to public authorities such as councils (not to Streetwave).

This privacy policy was prepared in August 2026. If you would like a prior version of this policy, or you have any questions about how we handle your personal data, please contact us using the details in section 1.3.