Sevenfire Research Limited 217 Strand, London WC2R 1AT · Company No. 10907452 · ICO registration ZB216818

Privacy Notice

Version 1.1 · Effective 23 October 2026 · Last reviewed 23 October 2026 · Owner: Michael Gregory, Chief Technology Officer (Responsible Person) · Approved by: Michael Gregory, Chief Technology Officer

1. Who we are and what this notice covers

Sevenfire Research Limited ("Sevenfire", "we", "us") trades as NPM (New Project Media) in the United Kingdom and is the controller of the personal data described in this notice. Our platform and business systems are operated on our behalf by our group company New Project Media Inc. ("NPM Inc."), in the United States, acting as our processor.

This notice covers personal data we hold about:

- the named platform users and account contacts of our subscribers;
- the people we deal with in business, including customers' staff, prospects, and conference and industry contacts; and
- people named in our editorial research, news and data on the energy industry.

NPM's website and events are covered by NPM's website privacy policy.

2. How to contact us

For any question about this notice or to exercise your rights, email **security@newprojectmedia.com** or write to Data Protection, Sevenfire Research Limited, 217 Strand, London WC2R 1AT.

We have not appointed a data protection officer. Responsibility for data protection sits with our Chief Technology Officer.

3. What we collect, why, and our lawful basis

What we do	Personal data	Why	Lawful basis
Platform accounts	Name, business email address, organization, job title, the content your subscription covers, your sign-in account (passwords are held only as a salted hash), account settings, and bulletin and	To provide, secure and administer the subscription your organization has bought for you	Legitimate interests: providing the service our customer has subscribed to for its people, and keeping it secure. Where you subscribe in your own name, performance of our contract with you

	alert preferences		
Platform use and security	Pages viewed, content accessed, API requests and their parameters, the delivery and opening of alert emails (including the IP address and browser details recorded when an email is opened or a link clicked), IP addresses of live connections, and application and service logs	To operate and secure the platform, investigate faults and misuse, and understand how subscriptions are used	Legitimate interests: running a reliable and secure service and improving it
Alert emails	Business email address and the alerts you have set up	To send the alerts you have chosen, and to stop sending to addresses that bounce	Legitimate interests: delivering the service you have asked for
Business relationships	Name, business email address, organization, job title, and our history of subscriptions, correspondence and event contact with you	To manage our relationships with customers, prospects and industry contacts, to administer subscriptions (including contracting and invoicing), and to tell you about our services and events	Legitimate interests: running and developing our business. Each marketing email lets you opt out, and you can opt out at any time by contacting us
Correspondence and documents	Business contact details and the content of emails and documents we exchange with you	To conduct our business and keep records of it	Legitimate interests: conducting our business and establishing or defending legal claims. Legal obligation, for records we must keep for accounting and tax

Product feedback	Your name and business email, your feedback, and a screenshot and short session replay of the page you were on, if you send feedback through the platform	To fix problems and improve the platform	Legitimate interests: improving our service
Editorial research	Names, job titles, employers, career moves, and professional activities and statements of people active in the energy industry	To research and publish news, analysis and data on energy markets and the people who shape them	Legitimate interests: publishing journalism and market information of public interest
AI features (only where your organization has enabled them)	The text you type into the platform's AI chat and the conversation history	To answer your questions	Legitimate interests: providing the features your organization has chosen
Data protection requests	The details of your request and how we handled it	To respond to your request and show that we did	Legal obligation

If you are a platform user, we need your name and business email address to give you access. Without them we cannot set up your account.

4. Where your data comes from

- **Platform users.** From the organization that subscribes for you, which tells our account managers who should have access, and from you when you use the platform.
- **Business contacts.** From you, from your employer in the course of our dealings with it, at conferences and industry events, and from public professional sources such as company websites.
- **Editorial research.** From public sources: company announcements and press releases, company websites, regulatory and corporate filings, conference materials and published media, and from our own reporting, including interviews. We tell the people named in our research about our processing through this notice rather than individually, because contacting each person would involve disproportionate effort.

5. Who we share it with

- **Our group companies.** NPM Inc. (United States) operates our platform and systems as our processor. New Project Media Australia Pty Ltd provides sales and support for subscribers in the Asia-Pacific region as our processor.

- **Service providers acting on our instructions**, for: cloud hosting and databases; search and analytics hosting; application monitoring; customer relationship management; email and documents; accounting and invoicing; IT managed services and backup of email and documents; and product feedback and issue tracking. A current list is available on request.
- **AI model providers**, only where an organization has enabled AI features. Our OpenAI and Google API usage is configured with logging disabled, and inputs and outputs are not used to train provider models. We do not hold zero-data-retention agreements: providers may retain inputs for a limited period for abuse and security monitoring under their standard paid API terms. Models run on Amazon Bedrock process inference within NPM's own AWS account.
- **Map tiles.** When you view a map in the platform, your browser loads map images directly from our mapping provider, which receives your IP address.
- **Others where needed:** our professional advisers, auditors and insurers; authorities where the law requires it; and a buyer or successor if all or part of our business is sold or reorganized.

We do not sell personal data.

6. International transfers

Our platform and business systems are hosted mainly in the United States. When personal data leaves the United Kingdom, we protect the transfer with one of the following safeguards:

- the UK Extension to the EU-U.S. Data Privacy Framework, where the recipient is certified under it;
- the UK International Data Transfer Agreement, which covers transfers to NPM Inc. and New Project Media Australia Pty Ltd;
- the European Commission's Standard Contractual Clauses with the UK Addendum; or
- UK adequacy regulations, for recipients in the European Economic Area.

Some administration of our systems is carried out by an engineering contractor outside the UK and the European Economic Area. Where a safeguard for a transfer is still being put in place, as it is for that access, you can ask us how the transfer is protected in the meantime.

You can ask us for details of the safeguard for any transfer using the contact details in section 2.

7. How long we keep it

We keep the personal data of platform users and business contacts under our Data Retention Schedule. In summary:

Personal data	How long
Platform accounts	While you have access. A removed user is permanently deleted on request, under our

	agreement with your organization, or after 24 months without access or use
Usage statistics and API request logs	Up to 24 months from the date recorded. Aggregated statistics that do not identify individuals, such as user counts by organization, may be kept for longer
Application and cloud service logs	15 days and up to 90 days
Business contacts	Until you opt out of contact or ask us to delete your details
Correspondence and documents	The duration of the business relationship and 6 years after it ends
Product feedback	12 months after the issue is closed
AI conversation history	The period set by your organization's administrator
Data protection request records	3 years after the request is closed
Editorial research	As part of our published archive
Backup copies	Platform data: no more than 65 days after deletion. Email and documents: up to 30 days after deletion

8. Your rights

You have the right to:

- access the personal data we hold about you;
- have inaccurate data corrected;
- have your data erased;
- restrict how we use your data;
- object to our use of your data where we rely on legitimate interests, and object at any time to direct marketing, which we will stop as soon as we log your request;
- receive data you gave us in a portable format, where we process it under a contract with you or your consent; and
- withdraw consent at any time, where we rely on it.

These rights have limits set by law. To use any of them, contact us as set out in section 2. We may need to confirm your identity first. We do not charge, unless a request is manifestly unfounded or excessive, and we respond within one month, which we may extend by up to two further months for complex requests; if we do, we will tell you why.

If you are unhappy with how we handle your data, please tell us. You can also complain to the Information Commissioner's Office at ico.org.uk or on 0303 123 1113.

9. Automated decisions

We do not make decisions about you based solely on automated processing that have legal or similarly significant effects on you.

10. Security

Personal data is encrypted in transit and at rest. Access to production systems is restricted to named administrators under NPM's Access Control Policy, and multi-factor authentication is required for all staff access to our development and production systems. Customer personal data is not used in development or testing.

11. Children

Our services are for professionals and are not directed at anyone under 18.

12. Changes to this notice

We review this notice at least once a year and whenever our processing changes. The version and review date at the top show when it last changed.

Document control

Version	Date	Change
1.0	14 October 2026	First Sevenfire privacy notice. For the personal data described in section 1, it supersedes NPM's website privacy policy (last updated February 2026), which continues to cover NPM's website and events
1.1	23 October 2026	Section 6: transfers where a safeguard is still being put in place. Section 10: multi-factor authentication wording

Owner: Michael Gregory, Chief Technology Officer (Responsible Person) · Approved by: Michael Gregory, Chief Technology Officer; version 1.0 ratified by the Chief Executive Officer on 14 October 2026; version 1.1 approved 23 October 2026 (interim approver) · Next review: 14 October 2027