Unrival — Privacy Notice

Version 4.4 | Dated: 1 May 2026

At a glance

Unrival Limited is a UK-based business intelligence research company. We carry out tightly-scoped research on a small number of named senior business contacts at organisations our customers are actively engaging with, so that our customers can have informed, relevant conversations with the right people. We do not aggregate data at scale. We do not sell consumer data. We do not collect or process email addresses, phone numbers, financial data, or any special categories of personal data.

If you have been told that you appear in research we have delivered to one of our customers — or if you believe you might — this notice tells you:

- what we hold (it is deliberately minimal);
- why we hold it and our lawful basis;
- how to exercise your rights, including the right to ask us for a copy of what we hold (a "subject access request") and the right to be removed from our research records;
- how to complain to us or to the regulator.

We aim to respond to any rights request within 30 days. Our contact is **privacy@unrival.net**.

Table of contents

1. Who we are

Unrival Limited (company number 07828657) is a private company incorporated in England and Wales, with registered office at 37th Floor, One Canada Square, Canary Wharf, London E14 5AA. We are the data controller for the personal data described in this notice, except where this notice expressly identifies another party as the controller.

Our Data Protection contact is reachable at **privacy@unrival.net**.

We are registered with the UK Information Commissioner's Office (which under the Data (Use and Access) Act 2025 will become the Information Commission).

2. What this notice covers

This notice covers two distinct sets of personal data we handle:

- **Headline Data** — minimal business-context information about a small number of named senior individuals at organisations our customers are engaging with. Sections 4 to 13 deal with this.
- **Customer and website data** — information we hold about our business customers (legal entities and their representatives), website visitors, and people who interact with us directly. Section 15 deals with this.

If you are reading this notice because you have been told your details appear in research delivered to one of our customers, **the parts that apply to you are Sections 3 to 13**.

This notice is governed by, and we comply with, the UK General Data Protection Regulation (as amended by the Data (Use and Access) Act 2025), the Data Protection Act 2018, and where applicable the EU General Data Protection Regulation (Regulation 2016/679) and equivalent national law.

3. The research service: in summary

Our customers — typically B2B technology, professional services, and financial services companies — engage us to produce **precision research** on a small number of named senior individuals at organisations they are actively in commercial dialogue with. A typical engagement covers between five and twenty named individuals at one target organisation, even where that organisation has tens of thousands of employees.

We do not crawl entire organisations. We do not build speculative databases of contacts in case anyone might find them useful in the future. We work to a specific, named, customer use case, and the data we produce is delivered to that customer and only that customer, in an environment provisioned exclusively for them.

This matters because UK and EU data protection law requires us to use the **minimum** data necessary for a clearly-defined purpose. Our model is built around that principle.

4. The data we hold about individuals researched for our customers ("Headline Data")

For each individual researched, we hold the following ("Headline Data") and no more:

- first name;
- last name;
- salutation / title (e.g. Dr., Ms., Mr.);
- job title;
- employer / company affiliation;
- role description, drawn from the individual's own public profile (typically their LinkedIn "About" or company-bio summary);
- tenure in their current role;
- a verified image, where the individual has chosen to make a publicly-available image of themselves available (for example on their company website, conference biography, or professional networking profile);
- where available, a LinkedIn Sales Navigator profile link;
- our internal subject ID, which allows us to action your rights requests;
- where applicable, limited professionally-disclosed personal context as described in Section 4A.

We do not collect, hold, infer, or provide to our customers:

- email addresses;
- telephone numbers;
- home or personal addresses;

- financial information of any kind;
- special categories of personal data — that is, information about racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, health data, sex life, or sexual orientation;
- criminal-offence data;
- information about your private life, family, or non-professional activities, except for limited, factual references to interests or hobbies that you have yourself chosen to disclose in a professional context (see Section 4A below);
- inferences drawn from your data about your personality, political views, vulnerabilities, or buying behaviour.

Every individual whose Headline Data we process has a **documented Legitimate Interests Assessment (LIA) and balancing record** prepared at the time of research, accessible to our customer via our secure delivery environment, and available to you on request. We describe the LIA framework in Section 6.

4A. Professionally-disclosed personal context

In some cases, our research may incorporate brief, factual references to interests, hobbies, or biographical detail that you have yourself chosen to disclose in a clearly professional context — for example, your current employer's official biography page, your own LinkedIn profile, a business-press interview in which you are the named subject, or a conference biographical introduction.

We include this information only where:

- you have demonstrably chosen to associate the information with your professional profile;
- the information is genuinely relevant to the business-engagement purpose of the research;
- the source is recent and we have verified that it relates to you specifically (and not to a namesake);
- the information would not directly or indirectly disclose information falling within the special categories of personal data, and we err on the side of exclusion in any case of doubt.

We do not include personal information drawn from your private social media accounts, third-party social media posts about you, inferences from photographs, or any source you have not yourself chosen to publish in a professional context.

Every item of professionally-disclosed personal context that we include in research deliverables is **source-cited**, so that you can trace it back to its origin if you make an access request.

5. Why we do not contact data subjects directly: our Article 14(5)(b) position

Under Article 14 of the UK GDPR, organisations that obtain personal data from sources other than the data subject themselves are generally required to provide that data subject with privacy information directly. Article 14(5)(b) provides an exception where direct notification would involve **disproportionate effort**.

We rely on this exception. We do so for the following documented reasons:

1. We deliberately do not collect contact data. We do not hold an email address or telephone number for any of the individuals we research. To notify each individual directly, we would first have to acquire contact data that is **more intrusive** than the Headline Data we actually process. The Information Commissioner's Office and the European Data Protection Board have both made clear that the effort and intrusiveness of acquiring new personal data, solely in order to discharge a notice obligation about less intrusive processing, is itself disproportionate.

2. The processing is minimal and low-impact. The Headline Data we hold is limited (see Section 4), drawn from publicly-accessible professional sources that the individual has typically chosen to publish about themselves, and used solely in a business-context for the purpose of supporting professional engagement between our customer and the individual's employer. We do not profile, score, rank, target, or rate individuals on personal characteristics.

3. The published notice is your route to information. This Privacy Notice, available at https://www.unrival.net/privacy-your-data, contains everything an Article 14 notice would contain. It is publicly indexed, searchable, and free to access at any time.

4. We carry out a Data Protection Impact Assessment. We maintain a Data Protection Impact Assessment (DPIA) at programme level addressing the "invisible processing" risk identified by the ICO, and we review it annually.

5. The right of access remains fully available. You retain the right to ask us for a copy of everything we hold about you, the right to ask for correction, and the right to ask for erasure — all described in Section 13. We respond to these requests within 30 days.

This is the architecture the ICO expects of organisations relying on Article 14(5)(b): a documented disproportionate-effort justification, a publicly-available privacy notice, a DPIA, and a working rights-exercise mechanism. We meet all four.

6. Our lawful basis: legitimate interests and the balancing test

Our lawful basis for processing Headline Data is **legitimate interests** under Article 6(1)(f) UK GDPR.

The legitimate interest is twofold:

- **Our own legitimate interest** in operating a precision-research service for our business customers;
- **Our customer's legitimate interest** in engaging with their existing or prospective business counterparties in an informed and relevant way, which is itself recognised as a legitimate interest in Recital 47 of the UK GDPR and consistent with new Article 6(11) UK GDPR (inserted by the Data (Use and Access) Act 2025), which clarifies that direct marketing and adjacent business-development activity can constitute a legitimate interest.

For each individual researched, we conduct a documented Legitimate Interests Assessment recording:

- **Necessity** — that the processing is necessary for the stated business purpose and that less-intrusive alternatives (e.g. processing only the employer organisation) would not achieve it;
- **Minimality** — that the data is restricted to the Headline Data definition in Section 4;
- **Public-domain provenance** — that the data is drawn from sources the individual has chosen to make professionally available;
- **Reasonable expectation** — that a senior business person who publishes their professional profile in public-domain channels would reasonably expect to be approached, in a business-context, by counterparties their organisation does business with;
- **Balancing test** — that the data subject's rights and freedoms are not overridden by the processing, having considered: the absence of contact data, the absence of profiling, the absence of any decision-making with legal or similarly significant effect, the absence of sensitive categories, the publicly-accessible nature of the data, and the availability of all data subject rights including erasure;
- **Professionally-disclosed personal context check** — where any item of personal-context information is included (see Section 4A), the LIA records: the source URL or citation, the source type, the date verified, confirmation that the source relates to this individual and not a namesake, the business relevance, and confirmation that no special-category data is implied;
- **Considered alternatives** — that the data subject's rights would not be better served by direct notification given the disproportionality analysis in Section 5.

The LIA is available to the data subject on request.

We do not rely on consent as the lawful basis for processing Headline Data; we therefore do not need to obtain or refresh consent, and there is no consent for you to withdraw. You retain the right to **object** to the processing at any time under Article 21 UK GDPR (see Section 13).

7. Sources of the data

The Headline Data we hold about you was obtained from one or more of the following publicly-accessible sources:

- the website(s) of your current and previous employers;
- your professional networking profile (typically LinkedIn);
- conference and event biographies, panel listings, and speaker pages;
- regulated public registers (for example Companies House);
- press releases, news articles, and industry publications;
- official corporate filings and disclosures.

We do not obtain data from data brokers, sold lists, leaked datasets, scraped contact databases, or social media sources that are not professionally-oriented and publicly indexed.

8. Recipients of the data

We disclose Headline Data only to:

- **the single Unrival customer** that has engaged us to produce research on the relevant target organisation. We do not share Headline Data between customers, we do not re-use research deliverables across customers, and we do not maintain a cross-customer database of researched individuals;
- **the sub-processors listed in Section 16**, who provide infrastructure and AI-inference services under data processing agreements and act on our documented instructions only;
- **prospective or new owners** in the event we sell, transfer, merge, or restructure parts of our business or our assets, or acquire other businesses. If a change happens to our business, the new owners may use Headline Data in the same way as set out in this privacy notice;
- **regulators, courts, or law enforcement**, where we are legally required to do so.

Once we disclose Headline Data to our customer as part of the agreed deliverables, our customer becomes an **independent controller** in respect of how they use that data going forward. They have their own obligations under data protection law and their own privacy notice. We assist them in handling any onward rights requests they receive, but we have no control over their downstream use.

9. Retention

We retain researched Headline Data for a maximum of **six (6) months** following completion of the relevant project. For longer-running engagements that include scheduled refresh cycles, the retention period runs from the end of the engagement. After the applicable period, we delete the data from our active systems. We retain a date-stamped audit copy for our own record-keeping (in case of subsequent rights requests or regulatory enquiries) but this audit copy is segregated, access-controlled, and not used for any further research purpose.

Where you exercise your right of erasure (see Section 13), we will delete the data sooner.

We retain the LIA documentation associated with each researched individual for as long as we retain the underlying Headline Data, plus a short audit period.

10. International transfers

We do not transfer Headline Data outside the United Kingdom or the European Economic Area. All of our research, storage, and AI inference is performed in UK or EU regions only:

- **Cloud infrastructure and storage**: Amazon Web Services EMEA SARL, in the AWS EU-West-1 (Ireland) and EU-West-2 (London) regions.
- **AI inference (research analysis, AI Chat, AI-generated briefings)**: Amazon Bedrock, in EU regions, providing managed access to Anthropic Claude, Amazon Nova, and Amazon Titan foundation models.
- **AI inference (text-to-speech accessibility features)**: Microsoft Azure OpenAI Service, in the Sweden Central region.

Transfers between the UK and the EEA are governed by the UK's adequacy decision for the EEA and the European Commission's adequacy decision for the UK. No additional transfer mechanism is required for these intra-region flows.

In the event we ever transferred personal data outside the UK/EEA in the future (we have no current plans to do so), we would only do so on the basis of an adequacy decision, the UK International Data Transfer Agreement / Addendum, Standard Contractual Clauses, or another lawful transfer mechanism, and we would update this notice in advance.

11. Artificial intelligence: what we use, what we do not do

We use generative AI as part of our research methodology and within our delivery environment, on an **inference-only** basis. Specifically, AI assists with:

- **Research support for our human researchers** — summarising and structuring publicly-available information; pattern recognition across publicly-disclosed corporate filings, press, and industry data; quality-assurance checks on our research outputs.
- **AI Chat within our delivery environment** — our customers can query our delivery environment using a conversational AI interface (the "AI Chat") to navigate the intelligence we have prepared for them. The AI Chat operates on a read-only basis against the research outputs already prepared by our human researchers; it does not introduce new personal data, and any output is restricted in scope to the same Headline Data described in Section 4.
- **AI-generated podcast briefings** — short audio summaries of research outputs, generated from the prepared written outputs, for our customers' on-the-go consumption.
- **Text-to-speech features** for accessibility within the delivery environment.

We do not:

- train, fine-tune, or otherwise improve any AI model using Headline Data, customer data, or any other personal data;
- send personal data to consumer-facing AI products or to free-tier AI services;
- run AI directly on our own infrastructure (all inference is via managed enterprise services — Amazon Bedrock and Microsoft Azure OpenAI Service — both of which contractually commit to no training on customer inputs and no retention of customer inputs beyond the API request, except for short-term abuse monitoring as set out in the respective provider terms);
- allow AI to make any decision about a data subject without human review.

Human oversight is mandatory. Every AI-assisted output prepared as part of our research is reviewed and validated by a human researcher before it is included in any customer deliverable. AI Chat and podcast features operate against this already-human-reviewed material. Our Senior ML Engineer is responsible for AI governance and is named in our internal AI Governance Framework.

You have the right to object to AI-assisted processing of your personal data; see Section 13.

12. Automated decision-making and profiling

We do not make decisions about you using solely automated processing that produce legal effects, or similarly significant effects, concerning you. Our research output is the product of human judgment, supported (but not replaced) by AI tooling.

We do not profile you in the sense of evaluating personal aspects of your personality, behaviour, preferences, vulnerabilities, or buying patterns. Our outputs describe your publicly-disclosed professional role, together with any limited professionally-disclosed personal context you have chosen to publish about yourself (see Section 4A).

13. Your rights — including how to make a subject access request or be removed

You have the following rights under the UK GDPR and the Data Protection Act 2018 in relation to any Headline Data we hold about you. Most of these rights apply free of charge; we will only ever charge a reasonable fee where a request is manifestly unfounded or excessive, and we will tell you in advance if we believe that to be the case.

Right	What it means in practice
Access (Article 15)	You can ask for a copy of the Headline Data we hold about you, the LIA we prepared, the sources we obtained the data from, the identity of the customer we delivered it to, and any related information. We respond within one month. Email **privacy@unrival.net**.
Rectification (Article 16)	If anything we hold about you is inaccurate or out of date, we will correct it promptly on request.
Erasure (Article 17)	You can ask us to delete your Headline Data. We will do so unless we have an overriding legitimate ground to retain it (which is rare), and we will explain in writing if we cannot comply. We instruct deletion from active systems within 30 days and complete deletion as soon as our technical systems permit.
Restriction (Article 18)	You can ask us to suspend processing of your data while a question (about accuracy, lawfulness, or an objection) is resolved.
Object (Article 21)	Because we process on the basis of legitimate interests, you have the right to object to the processing. If you object, we will stop processing unless we can demonstrate compelling legitimate grounds that override your rights and freedoms. In practice, we expect most objections to be honoured.
Object to AI processing	You can ask us not to use AI in connection with your Headline Data — including the research-support AI, AI Chat, and AI-generated podcast features described in Section 11. Given our human-review architecture, we can accommodate this without affecting our ability to respond to the underlying research request from our customer.

Portability (Article 20)	Where applicable, you have the right to receive your data in a portable format. Because we do not rely on consent, this right has limited practical application to Headline Data, but we will respect it where it does apply.
Complain to the regulator	See Section 19.

How to make a request

Email **privacy@unrival.net** with:

- the right you wish to exercise (e.g. "access" or "erasure");
- your name and any aliases you have used professionally (e.g. maiden name);
- your current and recent employers;
- if possible, the LinkedIn URL we are most likely to have indexed.

We will acknowledge your request promptly and respond fully within one calendar month. If your request is complex or you have made multiple requests, we may extend by a further two months and will let you know within the first month if so.

We may need to verify your identity before responding. Because we do not hold contact data for you, we may ask you to confirm details that would reasonably only be known to you (for example, your employment history details), or to provide other reasonable evidence. We aim to make this proportionate — we will not require ID documents unless absolutely necessary.

We will not refuse a request because it is "inconvenient." We will only refuse, in whole or in part, where the law permits us to do so (for example, where another individual's rights would be affected), and we will always tell you why.

14. Children

Our research service is exclusively focused on senior business professionals in their professional capacity. We do not knowingly research, hold, or process personal data of anyone under 18, and our research methodology actively filters against the inclusion of any individual identified as a minor. Our website is not directed to children.

15. The website and our customer relationships (a separate data flow)

This section covers personal data we hold about people who interact with us directly — visitors to our website, prospective customers, our business customers' representatives, and people who contact us. This is a separate data flow from the research service described in Sections 3 to 13.

The data we may hold about you in this context includes:

- **Identity data**: first name, last name, title;
- **Contact data**: business email, business phone, business postal address;
- **Transaction and financial data** (where you are a customer): payment information, billing records;
- **Technical data** (where you visit our website): IP address, browser type, time zone, operating system;
- **Profile and usage data**: interactions with our website and services;
- **Marketing and communications preferences**.

Lawful basis: performance of contract (where you are a customer); legitimate interests (running our business, communicating with you about services you have asked about); consent (for marketing communications by email or text, and for non-essential cookies); legal obligation (for accounting and tax records).

If you fail to provide personal data. Where we need to collect personal data by law, or under the terms of a contract with you, and you fail to provide that data when requested, we may not be able to perform the contract we have or are trying to enter into with you. In that case we may have to cancel a service you have with us, and we will notify you if this is the case.

Retention: we retain customer records for the duration of the relationship plus seven years (UK financial-record statutory minimum); marketing preferences until you opt out; website analytics for a limited period as set out in our cookie information.

Cookies: we use a small number of cookies on our website. You can refuse non-essential cookies via your browser settings or the consent control on our site.

Marketing: you can opt out of any marketing communications from us at any time by emailing **privacy@unrival.net** or using the unsubscribe link in our messages.

The rights described in Section 13 apply equally to data held under this section.

16. Sub-processors and third parties

We rely on the following sub-processors and partners to deliver our services:

Provider	Role	Location
Amazon Web Services EMEA SARL	Cloud compute, storage, infrastructure, and hosting of our customer delivery environments	EU (Ireland, UK)
Amazon Web Services EMEA SARL — Amazon Bedrock	Managed AI inference (Anthropic Claude, Amazon Nova, Amazon Titan) for research support, AI Chat, and AI-generated briefings	EU regions
Microsoft Ireland Operations Limited — Azure OpenAI Service	AI inference for accessibility text-to-speech	EU (Sweden Central)
Professional advisers (lawyers, accountants, auditors, insurers)	Professional services	United Kingdom
HM Revenue & Customs and other UK regulators	Statutory reporting	United Kingdom
Information Commissioner's Office (in future, the Information Commission)	Regulatory registration	United Kingdom

Each sub-processor is bound by a written data processing agreement that mirrors the relevant UK GDPR obligations: confidentiality, security, no use of customer data for the sub-processor's own purposes (including no model training where the sub-processor offers AI services), incident notification, and audit rights.

If we change this list, we will update this notice and notify customers in line with their contracts.

17. Security

Technical and organisational measures

We protect personal data using a combination of organisational and technical measures, including:

- AES-256 encryption at rest for all stored data;
- TLS 1.3 in transit for all data flows;
- AWS KMS-managed encryption keys with automated rotation;
- Role-based access controls under the principle of least privilege;
- Multi-factor authentication for all personnel accessing systems containing personal data;

- AWS GuardDuty continuous intelligent threat detection across our environments, with findings routed into our incident-response process;
- 24/7 incident-response capability with an average response time of 30 minutes for critical incidents;
- Annual risk assessment with quarterly internal review by our COO;
- Annual AWS Well-Architected Framework reviews against the security and operational excellence pillars;
- Mandatory annual data protection training for all staff;
- Background checks and confidentiality undertakings for all personnel.

Architecture and customer isolation

Our entire infrastructure operates on Amazon Web Services, using AWS-managed services in their default-secure configurations. Each customer's delivery environment is provisioned in a **dedicated AWS Organization established solely for that customer**, which provides organisation-level tenant isolation — rather than account-level, schema-level, or row-level multi-tenancy. As a result, no other customer's data, configuration, or operational events can intersect with another customer's environment.

Inherited assurance

The underlying AWS and Microsoft services on which we rely are covered by their providers' own attestations and certifications, including SOC 1, SOC 2 Type II, SOC 3, ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, and PCI DSS. The corresponding reports are available to us and, under the respective providers' standard non-disclosure terms, can be shared with our customers and (under NDA) prospective customers on request.

Breach notification

We will notify affected data subjects and the ICO of any personal data breach where the law requires us to do so, in accordance with the timeframes set out in the UK GDPR.

18. Changes to this notice

We review this notice at least annually and update it whenever there is a material change to our processing.

The current version is 4.4, dated 1 May 2026. Previous versions are available on request.

19. Contact and complaints

For all data protection enquiries, rights requests, and complaints to us:

Email: **privacy@unrival.net** Postal address: Data Protection, Unrival Limited, 37th Floor, One Canada Square, Canary Wharf, London E14 5AA, United Kingdom.

Our Data Protection function is overseen by our Chief Operating Officer.

Complaints to the regulator:

You have the right to complain to the **Information Commissioner's Office** (the UK supervisory authority for data protection, becoming the Information Commission under the Data (Use and Access) Act 2025) at any time.

Website: https://ico.org.uk Helpline: 0303 123 1113 Postal address: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF, United Kingdom.

We would appreciate the chance to address your concerns first, but we will not stand in the way of your right to go directly to the ICO.

If you are based in the EEA, you may also complain to your local supervisory authority.

20. Glossary

Controller — the organisation that determines the purposes and means of the processing of personal data.

Data Protection Impact Assessment (DPIA) — a structured risk assessment carried out before high-risk processing of personal data begins, identifying mitigations and documenting the controller's reasoning.

Headline Data — the limited set of business-context personal data we hold about individuals researched for our customers, as defined in Section 4.

Legitimate Interests Assessment (LIA) — a structured assessment that documents the lawful basis under Article 6(1)(f) UK GDPR for a particular processing activity, including the necessity test, the legitimacy test, and the balancing test against the rights and freedoms of the data subject.

Personal data — any information relating to an identified or identifiable natural person.

Processor — an organisation that processes personal data on behalf of, and on the documented instructions of, a controller.

Professionally-disclosed personal context — limited factual information about hobbies, interests, or biographical detail that the individual has themselves chosen to publish in a clearly professional context (e.g. corporate biography, business-press interview, conference biographical introduction, their own LinkedIn "About" section), as defined in Section 4A.

Special categories of personal data — racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, health data, sex life, or sexual orientation. We do not process these.

UK GDPR — the UK General Data Protection Regulation, being Regulation (EU) 2016/679 as saved into UK law by the European Union (Withdrawal) Act 2018 and amended by the Data Protection Act 2018 and the Data (Use and Access) Act 2025.