

FOUR AGENCY WORLDWIDE LIMITED

EXTERNAL PRIVACY NOTICE

October 2026

This notice explains how Four Agency Worldwide Limited collects and uses personal information in connection with its website, services, recruitment, marketing, business relationships, client work and approved technology. It also explains the choices and rights available to individuals.

The descriptions below are activity-specific. Four Agency's role may differ between engagements, and a supplementary notice may apply where another group company or client determines the purposes and means of a particular processing activity.

QUICK REFERENCE

Question	Answer
Controller	Four Agency Worldwide Limited for the processing described in this notice, unless another entity is identified for a specific activity.
Contact	dataprotection@four.agency OR +44 20 3920 0555
Applicable law	UK data protection law applies to the processing described here. EU, UAE, UAE free-zone or Saudi law may also apply where the relevant territorial and activity tests are met.
CRM and company matching	We use business contact information to manage relationships and may use controlled company-level partner matching and sharing as described in section 7.
AI-enabled tools	Personal information may be processed only through approved uses and subject to the controls described in section 11.
Your rights	See section 14. You may contact us or complain to the Information Commissioner's Office.

01 - ABOUT THIS NOTICE

This notice applies to website visitors, people who contact us, clients and prospective clients, business contacts, partners, people whose information is handled while we provide services to others, job applicants, and people affected by our marketing, campaign or technology-enabled activities.

It does not govern a third party's independent use of personal information. Links to third-party sites and services are provided for convenience; those organisations give their own privacy information.

We may provide additional information at the point of collection or before a materially different use begins. That more specific information should be read with this notice.

02 - WHO IS RESPONSIBLE FOR YOUR PERSONAL INFORMATION

The controller for the processing described in this notice is:

Organisation	Details
Four Agency Worldwide Limited	Registered in England and Wales, company number 05114815 Registered office: The Hickman Building, 2 Whitechapel Road, London E1 1FX ICO registration number: Z3111083

Four Agency Worldwide Limited works with other companies in the Four group. A group company is not automatically a controller simply because it is part of the group. Where another group company decides why and how personal information is used, or acts with us as a joint controller, we will identify that company in the relevant contract, campaign information or supplementary privacy notice.

The Four group companies covered by this notice may include the following. The relevant controller is the company that determines the purposes and essential means of the particular processing, not every company in the list:

Group company	Location or trading name
FCC Worldwide Limited	United Kingdom
Four Communications Limited	United Kingdom
Four Marketing & Media Limited	United Kingdom
Four Communications Group FZ-LLC	Abu Dhabi, United Arab Emirates
Four Colman Getty Limited	United Kingdom
Consolidated PR Limited	United Kingdom
Four MSA Limited	Trading as Four Health Media
Four Broadgate Mainland Limited	Trading as Four Broadgate
Four Cymru FBA Limited	Trading as Four Cymru
Four Health Communications Limited	United Kingdom

Four Rain Limited	Trading as Four Brand
Legend Engage Limited	Trading as Four Engage

Questions about which Four company is responsible for a particular activity may be sent to dataprotection@four.agency.

03 - HOW TO CONTACT US

Questions, rights requests and concerns can be sent to:

Channel	Details
Email	dataprotection@four.agency
Telephone	+44 20 3920 0555
Post	Data Protection Team, Four Agency Worldwide Limited, The Hickman Building, 2 Whitechapel Road, London E1 1FX

04 - WHICH DATA PROTECTION LAWS APPLY

Four Agency Worldwide Limited is established in the United Kingdom. The UK GDPR and the Data Protection Act 2018, as amended including by the Data (Use and Access) Act 2025, apply to the processing described in this notice.

EU GDPR does not apply merely because information relates to an EU citizen or resident. For a UK organisation without an EU establishment, it may apply to a particular activity if that activity concerns offering goods or services to people who are in the European Union or monitoring their behaviour there, or in another situation covered by Article 3 EU GDPR. We assess this for the relevant activity. Where EU GDPR applies and the law requires an EU representative, the representative's details will be provided in the relevant privacy information.

Additional laws may apply depending on where the relevant Four entity is established, where an individual is located and the processing concerned. This may include the UAE Federal Personal Data Protection Law or an applicable UAE free-zone data protection regime. The applicable UAE regime is assessed by reference to the establishment and licence of the entity carrying out or determining the processing.

The Saudi Personal Data Protection Law may apply to processing carried out in the Kingdom of Saudi Arabia and, in some circumstances, to processing outside the Kingdom relating to individuals residing or staying there. Where UAE or Saudi requirements apply, we will observe the applicable rules and provide supplementary local privacy information, contacts or rights information where required.

05 - WHAT PERSONAL INFORMATION WE USE AND WHY

The table summarises our main processing activities. The exact information and recipient will depend on the service, relationship and instructions involved. We use only the information that is reasonably necessary for the stated purpose.

Activity	Information and purpose	Lawful basis and typical recipients
Website operation	IP address, device, session and browsing information, together with information submitted through website forms. We use this to operate and secure the site and understand its use.	Legitimate interests in operating and improving our website; consent where required for non-essential cookies. Website, hosting, analytics and security providers.
Enquiries and customer service	Name, work contact details, organisation, enquiry, request and related correspondence. We use this to respond, provide information, investigate issues and support clients and prospective clients.	Legitimate interests in responding and providing effective service; contract steps where relevant. Service, communications and fulfilment providers where necessary.
Feedback and service improvement	Feedback, survey responses and information about interactions with our services. We use this to evaluate and improve our services, quality and client experience.	Legitimate interests in service evaluation and improvement. Approved survey, research and analytics providers.
Individual clients	Identity, contact and payment details; instructions, correspondence and service information. We use this to assess, enter into and deliver the engagement.	Contract steps and performance; legitimate interests; legal obligations. Fulfilment partners, advisers and service providers where necessary.
Corporate client contacts and other people involved in client work	Business contact, role, correspondence and information supplied or generated in service delivery. We use this to manage and deliver client work.	Legitimate interests in delivering services and managing the engagement; contract-related interests; legal obligations where applicable. Clients, approved

		suppliers, advisers and other project participants.
Recruitment	Contact details, CV, work and education history, application material, interview notes, right-to-work and adjustment information. We use this to assess applications and administer recruitment.	Steps before a contract; legitimate interests; legal obligations; employment-law conditions or explicit consent for special-category information where appropriate. Recruitment platforms, referees and advisers.
Marketing and events	Name, work details, preferences, attendance and engagement. We use this to send relevant communications, manage events and measure engagement.	Legitimate interests for appropriate business-to-business communications; consent where required by PECR or other law. Email, event and fulfilment providers.
Client insight and analysis	Information about interactions with our website, communications and services, including content viewed and engagement, where collected lawfully. We use this to understand needs, evaluate communications and improve services.	Legitimate interests in understanding and improving our services; consent where required for cookies, pixels or similar technologies. Analytics, communications and research providers.
Relationship management and CRM	Name, work contact details, employer, role, communications, meeting and relationship history, preferences, leads and opportunities. Sources may include you, colleagues, your organisation, referrals, public professional sources and approved event or data providers.	Legitimate interests in maintaining business relationships, responding, planning services and developing our business; contract steps where relevant. Our CRM and approved service providers.
Company-level partner matching and sharing	Selected organisation-level records may be compared with, or made available to, an approved partner. These may include company name, domain, company identifier,	Information about an incorporated company or other legal entity is generally not personal information. Where a record nevertheless

	corporate address, industry, size, account status and selected company-level opportunity, deal or pipeline information. Outputs may include overlap counts and selected matched or non-matching company records. We do not use or disclose individual contact records for this purpose.	relates to an identifiable person, we rely on legitimate interests in developing and managing corporate partnerships and opportunities, subject to necessity and safeguards. Approved matching providers and selected partner organisations receive information under documented connection rules.
Online advertising, audience planning and campaign delivery	Depending on the campaign: identifiers, audience attributes, professional information, device data, consent signals and campaign interactions. Some activities use pseudonymous identifiers or third-party segments; some return aggregate reporting only.	The basis and roles are assessed for each activity and may include consent, legitimate interests or client instructions. Clients, publishers, audience/data providers, advertising platforms and measurement providers.
Social media and customer-audience activity	Where lawfully used: hashed contact identifiers, audience criteria and engagement data to reach or exclude audiences and measure activity.	Consent where required and otherwise legitimate interests, subject to platform terms, transparency and an activity-specific assessment. Relevant social or advertising platform.
Business administration and compliance	Contact, payment, correspondence, due-diligence and transaction records. We use this for finance, governance, legal claims, risk, audit and compliance.	Legal obligations and legitimate interests in running and protecting the business. Banks, professional advisers, auditors, insurers, authorities and transaction counterparties.
Corporate transactions	Relevant business contact, contract, account and due-diligence information may be reviewed or	Legitimate interests in evaluating and completing a transaction; legal obligations

	disclosed in connection with a reorganisation, investment, merger, acquisition or sale.	where applicable. Professional advisers, funders, purchasers and transaction counterparties subject to appropriate confidentiality and data protections.
Approved AI-enabled tools	Limited content supplied for an approved task, which may include business contact details or document content. We use this to support drafting, summarisation, research, analysis or administration where appropriate.	The lawful basis follows the underlying task, commonly legitimate interests, contract performance or legal obligation. Approved technology providers and authorised users, subject to section 11.

If we wish to use personal information for a materially different and incompatible purpose, we will identify an appropriate legal basis and provide further information before that use begins where required.

06 - SPECIAL CATEGORY AND CRIMINAL OFFENCE INFORMATION

Information about health, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, genetic or biometric identification, sex life or sexual orientation receives additional protection. Criminal-offence information is also subject to specific safeguards.

We do not seek this information as a routine part of ordinary business contact management. It may arise, for example, in recruitment and workplace adjustments, or in specialised client work. Before using it, we identify both an Article 6 basis and an applicable Article 9 condition (and, where required, a Data Protection Act 2018 Schedule 1 condition and policy document). We apply access restrictions and data minimisation. Professional information about a healthcare professional is not automatically health data, but information that reveals an individual's health condition or behaviour may be special-category data.

07 - BUSINESS RELATIONSHIPS, CRM AND COMPANY MATCHING

We maintain business contact records so that we can understand our relationship with an organisation and its people, record communications, respond to requests, plan work, manage opportunities and avoid sending irrelevant or duplicate communications. We

may combine information supplied directly with professional information from referrals, event lists, a person's organisation and public business sources.

We may use company-level partner or account-matching services to compare selected organisation records in our CRM with organisation records that a client, supplier, referral source or commercial partner is permitted to use. We may also make selected company records available through an approved partner connection. We do this to identify shared or relevant companies, understand existing corporate relationships, coordinate account planning, co-selling or co-marketing, manage referrals, measure a partnership and identify or progress relevant business opportunities.

The information used for this purpose may include company name, domain, company identifier, corporate address, industry, size, account status and selected company-level opportunity, deal or pipeline information. We do not use partner-matching services to match or disclose individual contact records, named account owners, personal contact details, free-text communications or special-category information for this purpose. Matching populations are intended to cover incorporated companies and other legal entities; we take reasonable steps to exclude sole traders and unincorporated businesses.

Information about an incorporated company or other legal entity is generally not personal information. If an organisation record nevertheless relates to an identifiable individual, we treat it as personal information and apply the safeguards, lawful-basis assessment and rights described in this notice.

The information visible to another organisation depends on the approved connection, company population and field-level sharing rules. A partner may receive an aggregate overlap count, an organisation-level match or selected matched or non-matching company records. We do not provide unrestricted access to our entire CRM. Access is configured for the relevant connection and may be changed, suspended or withdrawn.

Company matching or sharing does not itself authorise either party to use personal information for an unrelated purpose or to send marketing contrary to applicable law or an individual's preferences. If we propose to introduce person-level matching or sharing, we will assess that activity separately and update our privacy information before it begins where required.

Before a partner connection is used, we assess the purpose, lawful basis, necessity, reasonable expectations, roles, supplier and partner terms, permitted data, visible fields, security, international transfers, retention and individual controls. We use partner-specific access rules and may stop or restrict a connection. If a service introduces materially different sources, purposes, outputs or disclosures, we will assess that change and update our privacy information where required.

You may object to processing based on legitimate interests. You can always object to direct marketing. We will maintain suppression information where necessary to respect an opt-out.

08 - OUR ROLE IN CLIENT CAMPAIGNS

Data protection roles are determined by what the parties actually decide and do for a specific processing operation; they are not assigned once for every client relationship or every programmatic campaign.

- We may be a processor where we handle personal information only on documented client instructions.
- We may be an independent controller where we determine our own purpose and essential means, for example for our business administration or some relationship management.
- We and another organisation may be joint controllers where we jointly determine the purposes and essential means of a particular activity. Where required, we will put in place a transparent arrangement allocating responsibilities and make its essence available to affected people.
- Audience, media, publisher, data and platform providers may be processors, independent controllers or joint controllers depending on the activity and contractual reality. Their own privacy information may also apply.

Where a campaign uses marketplace segments or platform audiences, the data accessible to us varies. Some services expose individual-level or pseudonymous records; others provide only selection tools and aggregate reporting. We will describe the relevant arrangement rather than assume that we never receive or access underlying personal information.

09 - WHERE PERSONAL INFORMATION COMES FROM AND WHO RECEIVES IT

We collect information directly from individuals and may also obtain it from clients, employers, colleagues, referrals, event organisers, recruitment platforms, public professional sources, audience or data providers, advertising and social platforms, technology partners and other suppliers. Where Article 14 UK GDPR applies, we provide source and category information within the required period unless a lawful exception applies.

Recipients may include other Four group companies involved in the relevant service, clients and project partners, CRM and technology providers, fulfilment and production partners, hosting and security providers, analytics and advertising platforms, professional advisers, insurers, auditors, authorities, prospective purchasers and other recipients required for a corporate transaction. We limit access according to role and purpose.

10 - INTERNATIONAL TRANSFERS

Some recipients or their service locations may be outside the United Kingdom. Where a disclosure is a restricted transfer under UK GDPR, we use a lawful transfer route appropriate to that transfer. This may include UK adequacy regulations, an International Data Transfer Agreement, the UK Addendum to EU Standard Contractual Clauses, approved binding corporate rules or an applicable exception. Where a safeguard requires it, we carry out and document a transfer risk assessment (also referred to in UK law as the data protection test) and add supplementary measures where necessary.

For personal information governed by EU GDPR, the relevant EU transfer rules apply separately, including EU adequacy decisions or EU Standard Contractual Clauses where appropriate. A provider's participation in a recognised framework is relied upon only after its current status and coverage have been checked.

Where the UAE Federal Personal Data Protection Law, an applicable UAE free-zone regime or the Saudi Personal Data Protection Law governs a transfer, we apply the transfer conditions, safeguards, assessments and approvals required by that regime. A transfer route valid under UK law is not assumed to satisfy another jurisdiction's requirements.

You may contact us for more information about the transfer route and to request a copy of relevant safeguards, subject to necessary redactions.

11 - USE OF AI-ENABLED TOOLS

Data protection law applies when an AI-enabled tool processes personal information. The 2026 regulations concerning an AI and automated-decision-making code of practice require the Information Commissioner to prepare guidance; they do not by themselves establish that every use of AI is lawful or impose a single operational rule for all organisations.

We may use approved AI-enabled tools to support tasks such as drafting, editing, summarising, research, analysis and administration. The information supplied must be limited to what is necessary for the approved task. Special-category or confidential client information requires specific authorisation and safeguards.

The status of an AI provider depends on the service and terms. Before an approved use involving personal information, we assess the provider, purpose, lawful basis, access, retention, security, transfer arrangements and contract. We select account settings and contractual options intended to limit secondary use, including model training, where available and appropriate. We do not state that every provider acts only as our processor or that every service excludes training unless the applicable terms and configuration support that statement.

Where solely automated processing is used to make a decision that has a legal or similarly significant effect, we will provide the information and safeguards required by UK GDPR, including an opportunity to make representations, obtain human intervention and contest the decision. We will conduct a data protection impact assessment where the processing is likely to result in a high risk to individuals.

12 - HOW WE PROTECT PERSONAL INFORMATION

We use technical and organisational measures designed for the nature and risk of the processing. These may include role-based access, authentication, encryption where appropriate, supplier due diligence, contractual controls, secure configuration, backups, logging, staff training, incident management and periodic review.

Where a supplier processes personal information on our behalf, we put in place the contract required by Article 28 UK GDPR before that processing begins. Some third parties are independent or joint controllers rather than processors; the appropriate controller arrangements apply to those relationships.

We assess personal data breaches and notify the ICO without undue delay and, where feasible, within 72 hours after becoming aware of a breach when UK GDPR requires notification. Where a breach is likely to result in a high risk to individuals, we also communicate it to affected people unless an exception applies.

13 - HOW LONG WE KEEP PERSONAL INFORMATION

We keep personal information only for as long as necessary for the purposes described, including to meet legal, accounting, audit, insurance and regulatory requirements, deal with complaints and establish, exercise or defend legal claims. The applicable period is set in our retention schedule or the relevant client or project instructions and is reviewed when the purpose or law changes.

Category	How the period is determined
Enquiries and business relationships	For as long as needed to respond, follow up and manage the relationship; afterwards, only for a period justified by complaints, potential claims, audit needs and suppression requirements.
Client and project records	For the engagement and afterwards only for periods justified by contractual, professional, tax, insurance, audit and legal-claim requirements; documented client instructions apply where we act as processor.
Recruitment	For the recruitment process and afterwards for a period justified by recruitment follow-up and potential claims. Successful applicants' records move to the relevant employment retention schedule.

Marketing and events	Until consent is withdrawn, an objection is made, the purpose ends, or an approved inactivity rule is met. Minimal suppression data may be kept to respect opt-outs.
CRM and company matching	While the record supports an active or reasonably anticipated business relationship, subject to periodic inactivity and accuracy review. Source records follow their applicable category; company-matching inputs and outputs are retained only for the approved purpose, audit or dispute needs and configured deletion rule.
Technology and AI-enabled processing	According to the approved task, contract, account configuration and retention schedule. Temporary prompts, outputs and logs are not assumed to have one universal period.
Compliance and finance	For the period required by applicable company, tax, anti-fraud, regulatory and legal-claims obligations.

At the end of the applicable period, information is securely deleted or anonymised unless a lawful reason requires continued retention.

14 - YOUR RIGHTS

Depending on the circumstances, you may have the following rights. Rights are not absolute, and an exemption may apply. We normally respond within one month after receiving a valid request, subject to any lawful extension or pause while required information is obtained.

If UAE, UAE free-zone or Saudi data protection law applies to your information, you may also have rights under that law. We will explain any materially different local right, response period or regulator contact in supplementary information where required.

Right	What it means
Access	Ask whether we process your personal information and receive a copy and related information.
Rectification	Ask us to correct inaccurate information or complete incomplete information.
Erase	Ask us to delete information in circumstances set out by law.
Restriction	Ask us to restrict processing in specified circumstances.
Portability	Receive information you provided in a structured, commonly used and machine-readable format where processing is automated and based on consent or contract, and ask for transmission where technically feasible.
Object	Object to processing based on legitimate interests or a public task. You have an absolute right to object to direct marketing.
Withdraw consent	Withdraw consent at any time where processing relies on consent, without affecting earlier lawful processing.

Automated decisions	Where Article 22C UK GDPR applies, receive information, make representations, obtain human intervention and contest the decision.
Complain	Make a data protection complaint to us and make a complaint to the Information Commissioner's Office. If EU GDPR applies, you may also have the right to complain to the competent EU supervisory authority.

ICO complaints: ICO complaint form OR 0303 123 1113

You may make a data protection complaint to us using the contact details in section 3. We will acknowledge a complaint within 30 days and, without undue delay, make appropriate enquiries, keep you informed where necessary and tell you the outcome, as required by section 164A of the Data Protection Act 2018.

15 - CONSENT AND COMMUNICATION PREFERENCES

Where we rely on consent, you can give it through the mechanism presented when information is collected or by contacting us. You may withdraw consent at any time. Withdrawal does not affect processing carried out lawfully before withdrawal. You can also change marketing preferences or object to direct marketing using the unsubscribe or preference controls provided in a communication, or by contacting us.

16 - COOKIES AND SIMILAR TECHNOLOGIES

Our website may use cookies, pixels, tags, local storage and similar technologies to operate, secure and improve the site, remember preferences, measure use and support advertising. Strictly necessary technologies do not require consent. We use non-essential analytics, functionality or advertising technologies only where the required consent or other lawful permission has been obtained.

Current details and controls are provided in our Cookie Policy: four.agency/legal-and-privacy

17 - THIRD PARTY CONTRACTORS AND OTHER CONTROLLERS

We use third-party contractors and service providers where they are needed to operate our business or deliver services. Depending on the activity, these may include hosting and IT providers, CRM and communications platforms, analytics and security providers, marketing and event suppliers, recruitment services, research and audience providers, fulfilment and production partners, payment and finance providers, professional advisers and approved AI-enabled technology providers.

Where a supplier processes personal information only on our behalf, it acts as a processor. We carry out proportionate due diligence and put in place the contract required by Article 28 UK GDPR. That contract addresses documented instructions, confidentiality, security, sub-processors, assistance with rights and incidents, and the return or deletion

of information as applicable. We monitor or review the arrangement in proportion to its risk.

We may also disclose or make personal information available to organisations acting as independent or joint controllers. These may include other Four group companies, clients, project and referral partners, partner-matching participants, event organisers, publishers, audience or data providers, advertising and social platforms, banks, insurers, professional advisers, regulators, public authorities and parties involved in a corporate transaction.

Roles depend on the decisions made for the specific activity. Independent controllers determine their own purposes and are responsible for their own compliance and privacy information. Where we jointly determine purposes and essential means with another organisation, we put in place the transparent arrangement required by Article 26 UK GDPR and make its essence available where required. A data-sharing or controller arrangement does not remove any controller's legal responsibilities.

Our website and communications may link to third-party websites or services. We do not control their independent processing and encourage you to read their privacy information.

18 - CHANGES TO THIS NOTICE

We review this notice periodically and update it when our processing, legal requirements or services materially change. We will bring material changes to people's attention in an appropriate way before a new use begins where required.

Version date: 23 October 2026. On publication, this version replaces the notice dated November 2024.

APPENDIX - KEY TERMS

Term	Meaning
Controller	The organisation that determines the purposes and essential means of processing personal information.
Processor	An organisation that processes personal information on a controller's documented instructions.
Joint controllers	Two or more organisations that jointly determine the purposes and essential means of a processing activity.
Personal information	Information relating to an identified or identifiable living individual; also called personal data.
Special category information	Personal information given additional protection under Article 9 UK GDPR.
CRM	A customer or relationship management system used to organise business contacts, interactions, leads and opportunities.
Company matching and sharing	A controlled comparison or exchange of selected organisation-level records under approved connection, company-population and field-level rules. It may identify overlaps or make permitted matched and non-matching company records available for an approved partnership purpose.
Pseudonymised	Processed so that information cannot be attributed to a person without additional information kept separately and protected.
Anonymous	Information that does not relate to an identified or identifiable person. Pseudonymous information is still personal information.
PECR	The Privacy and Electronic Communications Regulations, which include rules for electronic marketing and cookies.
DPIA	A data protection impact assessment used to identify and reduce high privacy risks before processing begins.

Contact: dataprotection@four.agency | +44 20 3920 0555