

THE TELECOMS ADVOCATE LTD

PRIVACY POLICY

Version: 2.4

Effective Date: 6 August 2026

1. ABOUT THIS PRIVACY POLICY

The Telecoms Advocate Ltd is committed to handling personal data lawfully, fairly, transparently and securely.

This Privacy Policy explains:

- a) what personal data we collect;
- b) where we obtain it;
- c) why and how we use it;
- d) the lawful bases upon which we rely;
- e) who we may share it with;
- f) how long we retain it;
- g) how we protect it; and
- h) the rights available to individuals.

This Policy applies to personal data relating to:

- a) Clients and prospective Clients;
- b) directors, employees, partners and representatives of Clients;
- c) individuals who authorise us to exercise data-protection rights on their behalf;
- d) individuals whose information appears in documents or evidence connected with a Matter;
- e) suppliers, introducers, professional advisers and business contacts;
- f) people who communicate with us or make a complaint; and

g) users of our website and online services.

This Policy should be read alongside our General Terms and Conditions, Engagement Agreement and any matter-specific agreement.

2. WHO WE ARE

Company: The Telecoms Advocate Ltd

Company Number: 16694159

VAT Number: 515 3574 95

Registered Office: 124–128 City Road, London EC1V 2NX

Website: www.thetelecomsadvocate.com

Email: contact@thetelecomsadvocate.com

Telephone: 02031 431390

ICO Registration Reference: ZC058993

The Telecoms Advocate Ltd is registered with the Information Commissioner's Office under the organisation name:

THE TELECOMS ADVOCATE LTD

Our registration reference is:

ZC058993

Registration records TTA's entry on the ICO's register and should not be interpreted as certification, endorsement or approval by the ICO of any particular service or processing activity.

The Telecoms Advocate Ltd is referred to in this Policy as "**TTA**", "**we**", "**us**" or "**our**".

For most personal data processed in connection with our services and business operations, TTA acts as the **data controller**. This means that we determine why and how that personal data is used.

In limited circumstances, TTA may process personal data on behalf of another organisation. Where TTA acts as a data processor, the parties' respective responsibilities will be governed by an appropriate written agreement.

Whether an organisation acts as controller or processor depends upon the purposes of the processing and the degree of control exercised in practice.

3. DATA-PROTECTION LAWS

We process personal data in accordance with applicable UK data-protection and privacy law, including:

- a) the UK General Data Protection Regulation;
- b) the Data Protection Act 2018;
- c) the Data (Use and Access) Act 2025;
- d) the Privacy and Electronic Communications Regulations 2003, where applicable; and
- e) other applicable legislation and regulatory requirements.

The Data (Use and Access) Act 2025 amended parts of the UK data-protection framework, with relevant changes taking effect in stages between June 2025 and June 2026.

4. PERSONAL DATA WE MAY COLLECT

The personal data we collect depends upon our relationship with you and the nature of the Matter.

4.1 Identity and contact information

This may include:

- a) names;
- b) job titles and positions;
- c) business and trading names;
- d) postal addresses;
- e) email addresses;
- f) telephone numbers;

- g) signatures;
- h) company or registration details; and
- i) identification documents where reasonably required.

4.2 Client and Matter information

This may include:

- a) details of telecommunications products and services;
- b) contract, order and account information;
- c) telephone numbers and service identifiers;
- d) billing and payment information;
- e) equipment, rental, lease or finance information;
- f) complaint and dispute histories;
- g) correspondence with providers, resellers, brokers, funders or lessors;
- h) notes of telephone calls, meetings and events;
- i) witness accounts and statements;
- j) evidence concerning the procurement, supply, operation or termination of services;
- k) information about alleged loss, liability or commercial impact;
- l) proposed or completed settlements;
- m) ADR, regulatory or court-related information; and
- n) documents prepared by us or supplied to us in connection with the Matter.

4.3 Information concerning other individuals

Documents connected with a Matter may contain personal data relating to:

- a) directors;
- b) employees;
- c) contractors;

- d) customers;
- e) sales representatives;
- f) provider personnel;
- g) witnesses;
- h) professional advisers;
- i) family members; or
- j) other individuals connected with the underlying events.

Clients should provide only information which is reasonably relevant and which they are lawfully entitled to disclose.

4.4 Financial and transaction information

This may include:

- a) invoicing details;
- b) payments made to or by TTA;
- c) bank details where reasonably required;
- d) account credits or refunds;
- e) financial outcomes;
- f) tax and VAT information; and
- g) records required for accounting, debt recovery or audit purposes.

We do not ordinarily retain complete payment-card information where payments are handled through a specialist payment provider.

4.5 Communications and call information

We may process:

- a) emails;
- b) letters;
- c) messages;

- d) telephone notes;
- e) voicemail messages;
- f) meeting records;
- g) call recordings; and
- h) communications made through our website, case-management system or other approved platforms.

4.6 Technical and website information

Where applicable, we may collect:

- a) internet protocol addresses;
- b) browser and device information;
- c) website usage information;
- d) login and security records;
- e) cookie identifiers;
- f) access logs; and
- g) information submitted through online forms.

4.7 Complaint and rights-request information

We may process information concerning:

- a) complaints about our services;
- b) data-protection complaints;
- c) subject access requests;
- d) requests for correction, deletion, restriction or objection;
- e) identity verification; and
- f) correspondence with the Information Commissioner's Office or another authority.

5. WHERE WE OBTAIN PERSONAL DATA

We may obtain personal data:

- a) directly from you;
- b) from the Client or its Authorised Contact;
- c) from an individual who has authorised us to act in connection with a subject access request;
- d) from providers, resellers, brokers, suppliers, funders, lessors and assignees;
- e) through correspondence, disclosure or account records;
- f) from solicitors, barristers, accountants, insurers and other professional advisers;
- g) from ADR schemes, regulators, courts or public authorities;
- h) from publicly available registers, websites or records;
- i) from introducers or referral partners;
- j) through call recordings or meeting notes; and
- k) through approved IT, communications or case-management systems.

Where personal data is obtained from someone other than the individual concerned, we will provide appropriate privacy information where required.

Where applicable, that information will ordinarily be provided:

- a) within a reasonable period and no later than one month after obtaining the personal data;
 - b) at the time of our first communication with the individual; or
 - c) before the personal data is first disclosed to another recipient,
- whichever applies first.

This is subject to the exemptions and exceptions permitted by data-protection law, including where the individual already has the information or providing it would be impossible or involve disproportionate effort.

6. HOW AND WHY WE USE PERSONAL DATA

6.1 Enquiries and onboarding

We may use personal data to:

- a) respond to enquiries;
- b) assess whether we may be able to assist;
- c) verify Client identity, legal status and authority;
- d) carry out conflict, compliance or risk checks;
- e) prepare engagement documents;
- f) establish a Client file; and
- g) issue invoices and arrange payment;
- h) allocate the Matter internally and reserve initial professional capacity; and
- i) manage onboarding, case allocation and related Fees.

6.2 Delivering our services

We may use personal data to:

- a) investigate a Matter;
- b) identify relevant parties and agreements;
- c) obtain and review evidence;
- d) prepare Information and Evidence Requests;
- e) assist authorised individuals with subject access requests;
- f) analyse contracts, bills, correspondence and records;
- g) prepare Confidential Advice Reports;
- h) prepare correspondence, complaints, submissions and supporting documents;
- i) provide strategy, drafting and negotiation support;
- j) assist with ADR or professional referral;
- k) record instructions, work undertaken and outcomes; and

l) communicate with Clients and relevant third parties.

6.3 Business administration

We may use personal data to:

- a) manage Client relationships;
- b) allocate and supervise work;
- c) maintain case and accounting records;
- d) manage invoices and debts;
- e) obtain insurance or professional advice;
- f) assess and improve service quality;
- g) train and support personnel;
- h) manage complaints;
- i) maintain business continuity; and
- j) protect our legal, commercial and regulatory position.

Where reasonably practicable, website and service analytics will be aggregated or anonymised so that individuals are not directly identifiable.

6.4 Security, fraud prevention and legal compliance

We may use personal data to:

- a) verify identity and authority;
- b) protect our systems and communications;
- c) detect or investigate fraud, impersonation or unauthorised access;
- d) comply with court orders and lawful requests;
- e) respond to regulators and law-enforcement bodies;
- f) establish, exercise or defend legal rights;
- g) comply with tax, accounting and company-law obligations; and
- h) maintain records demonstrating compliance.

6.5 Marketing and business development

Where lawful, we may use business contact information to:

- a) provide information about relevant TTA services;
- b) maintain relationships with existing or former Clients;
- c) communicate with introducers and professional contacts;
- d) invite feedback; and
- e) provide relevant business or industry updates.

Individuals may opt out of marketing communications at any time.

We will not send electronic marketing or make marketing calls where applicable law requires consent unless the necessary consent has been obtained.

7. LAWFUL BASES

We identify an appropriate lawful basis before processing personal data. The basis used depends upon the purpose and circumstances.

Our purposes, lawful bases, retention periods and recipients form part of the privacy information which we are required to provide.

7.1 Contract

We may process personal data where it is necessary:

- a) to take steps at an individual's request before entering into a contract; or
- b) to perform a contract with that individual.

This basis may apply where the Client is a sole trader or where an individual personally enters into an agreement with TTA.

7.2 Legitimate interests

We may rely upon legitimate interests where processing is necessary for our legitimate business purposes, or those of a Client or third party, provided that those interests are not overridden by the individual's rights and freedoms.

Relevant legitimate interests may include:

- a) providing services to a corporate Client;
- b) investigating and resolving commercial disputes;
- c) communicating with Client representatives and relevant third parties;
- d) obtaining and evaluating evidence;
- e) preparing advice and strategic documents;
- f) administering our business;
- g) maintaining appropriate records;
- h) ensuring quality and accountability;
- i) preventing fraud and protecting information security;
- j) managing and recovering Fees;
- k) handling complaints; and
- l) establishing, exercising or defending legal rights.

We consider whether the processing is necessary, proportionate and within what the individual might reasonably expect.

7.3 Legal obligation

We may process personal data where necessary to comply with a legal obligation, including obligations relating to:

- a) tax and accounting;
- b) company records;
- c) data-protection rights;
- d) court orders;
- e) regulatory requirements; and
- f) lawful requests from public authorities.

7.4 Consent

We may rely upon consent where the law requires it or where consent is the most appropriate basis.

Where consent is relied upon:

- a) it will be requested clearly;
- b) it may be withdrawn at any time; and
- c) withdrawal will not affect processing already carried out lawfully.

We do not ordinarily rely upon consent where another lawful basis more accurately reflects the service relationship.

7.5 Establishing, exercising or defending legal rights

We may process personal data where necessary to establish, exercise or defend legal rights, resolve disputes or protect the legal interests of TTA, a Client or another relevant person.

For ordinary personal data, we will rely upon an applicable Article 6 lawful basis, such as legitimate interests, contract or legal obligation.

Where special-category or criminal-offence information is involved, we will also identify any additional condition required under the UK GDPR and the Data Protection Act 2018.

7.6 Information required to provide our services

Some personal data may be required so that we can:

- a) verify identity or authority;
- b) enter into and administer an engagement;
- c) investigate a Matter;
- d) prepare or submit an Information and Evidence Request;
- e) comply with legal obligations; or
- f) provide the requested Services.

Where necessary information is not provided, we may be unable to:

- a) accept an instruction;
- b) submit a request;

- c) complete an investigation;
 - d) prepare the CAR;
 - e) undertake further work; or
 - f) continue acting.
-

8. SPECIAL-CATEGORY AND CRIMINAL-OFFENCE DATA

A Matter may occasionally contain particularly sensitive information, including information concerning:

- a) health or disability;
- b) racial or ethnic origin;
- c) religious or philosophical beliefs;
- d) trade-union membership;
- e) sexual life or sexual orientation;
- f) biometric or genetic information; or
- g) alleged or proven criminal offences.

Clients should not provide sensitive information unless it is genuinely relevant and lawfully disclosed.

Where we process special-category personal data, we will identify:

- a) an Article 6 lawful basis; and
- b) an applicable Article 9 condition.

Depending upon the circumstances, the Article 9 condition may include:

- a) explicit consent;
- b) information manifestly made public by the individual; or
- c) processing necessary for the establishment, exercise or defence of legal claims.

Special-category processing requires both an Article 6 lawful basis and a separate Article 9 condition.

Where criminal-offence data is processed, we will identify an applicable condition under the Data Protection Act 2018 or another lawful authority.

We will maintain any additional policy documentation required by law.

9. SUBJECT ACCESS REQUESTS UNDERTAKEN FOR CLIENTS

As part of our Services, TTA may assist an authorised individual to prepare or submit a subject access request to another organisation.

A subject access request concerns an identifiable individual's personal data. It is not a general right for a company or other organisation to obtain every commercial document held by another organisation.

Where we assist with a subject access request:

- a) the individual must provide appropriate authority;
- b) identity evidence may be required;
- c) the request may be submitted by TTA or prepared for the individual to submit;
- d) personal data received may include information about other individuals;
- e) information may lawfully be withheld or redacted by the recipient; and
- f) TTA will use the resulting information only for the authorised Matter and related lawful purposes.

10. CALL RECORDING

We may record telephone or online calls for purposes including:

- a) confirming instructions;
- b) maintaining an accurate record of events;
- c) quality assurance;

- d) training and supervision;
- e) complaint handling;
- f) preventing misunderstanding or fraud;
- g) protecting Clients and TTA; and
- h) establishing, exercising or defending legal rights.

Callers may be informed that calls may be recorded by:

- a) a recorded message;
- b) verbal notification;
- c) written onboarding information;
- d) our Terms or Engagement Agreement; or
- e) another appropriate notice.

The applicable lawful basis will ordinarily be legitimate interests, contract or processing connected with the establishment, exercise or defence of legal rights, depending upon the circumstances.

Recordings will be accessible only to people who reasonably require access and will be retained in accordance with Section 15.

11. ARTIFICIAL-INTELLIGENCE-ASSISTED TOOLS

TTA may use approved artificial-intelligence-assisted or automated tools to support limited functions such as:

- a) document organisation;
- b) transcription;
- c) identifying potentially relevant material;
- d) summarisation;
- e) research assistance;

- f) drafting support;
- g) quality checking; and
- h) administrative efficiency.

Where personal data is processed using an AI-assisted tool, TTA will take reasonable and proportionate steps to:

- a) minimise the personal data used;
- b) restrict access;
- c) assess confidentiality and security risks;
- d) use appropriate business, contractual and privacy settings;
- e) verify material outputs through human review;
- f) avoid relying upon AI-generated content without professional assessment;
- g) prevent unauthorised secondary use;
- h) assess any relevant international transfer; and
- i) not knowingly permit identifiable Client Matter information to be used to train a public or general-purpose artificial-intelligence model.

Where an approved service provider processes information through an AI-assisted function, TTA will use reasonable contractual, technical and account-level controls to prevent unauthorised model training or secondary use.

TTA does not use AI systems to make solely automated decisions about a Client or individual which produce legal or similarly significant effects.

Any material use of personal data within an AI system remains subject to the data-protection principles, including lawfulness, fairness, transparency, accuracy, security and accountability.

12. WHO WE MAY SHARE PERSONAL DATA WITH

We may share personal data, where reasonably necessary and lawful, with:

- a) TTA employees, caseworkers, consultants and contractors;

- b) approved IT, email, cloud-storage, e-signature, communication and case-management providers;
- c) accountants, auditors and payment-service providers;
- d) insurers and insurance advisers;
- e) solicitors, barristers, experts and other professional advisers;
- f) providers, resellers, brokers, funders, lessors, assignees and other parties connected with the Matter;
- g) ADR schemes and complaint bodies;
- h) regulators and public authorities, including Ofcom and the Information Commissioner's Office where relevant;
- i) courts, tribunals and law-enforcement organisations;
- j) debt-recovery providers; and
- k) another person where the individual has authorised disclosure or the law otherwise permits it.

Where we propose to refer a Matter to an independent solicitor, barrister or other professional, we will obtain the Client's authority before sharing identifiable Matter information, unless disclosure is otherwise required or clearly permitted by law.

Any authority to share the CAR or other restricted Work Product is also subject to the contractual confidentiality, intellectual-property and restricted-use provisions in the applicable Engagement Agreement and General Terms.

Initial discussions concerning a possible referral may take place on an appropriately anonymised basis.

Anyone working for or on behalf of TTA who has access to personal data must be subject to appropriate confidentiality, security and data-protection obligations.

We do not sell or rent personal data to advertisers or unrelated third parties.

13. INTERNATIONAL TRANSFERS

Some IT, communications, storage or professional-service providers may process or make personal data accessible outside the United Kingdom.

Before making a restricted international transfer, we will take reasonable steps to ensure that an appropriate transfer mechanism and safeguards are in place.

Depending upon the destination and recipient, this may include:

- a) UK adequacy regulations;
- b) the UK International Data Transfer Agreement;
- c) the UK Addendum to approved contractual clauses;
- d) another legally recognised transfer mechanism;
- e) supplementary contractual or technical protections; and
- f) an appropriate transfer-risk assessment.

The UK GDPR contains specific requirements for restricted transfers of personal data outside the United Kingdom.

Further information about safeguards used for a relevant transfer may be requested from TTA.

14. INFORMATION SECURITY

We take reasonable and proportionate technical and organisational measures to protect personal data against:

- a) unauthorised access;
- b) unlawful use or disclosure;
- c) accidental loss;
- d) alteration;
- e) destruction;
- f) malware and cyberattack; and
- g) inappropriate retention.

Measures may include:

- a) access controls;
- b) password protection;
- c) multi-factor authentication;
- d) encryption where appropriate;
- e) secure cloud systems;
- f) role-based access;
- g) confidentiality obligations;
- h) personnel and contractor training;
- i) secure document-transfer procedures;
- j) backup and recovery measures;
- k) supplier due diligence; and
- l) incident-management procedures.

No electronic system is completely secure.

Individuals should avoid sending unnecessary sensitive information through insecure channels and should verify any apparent change to TTA's payment details using a known telephone number.

Where a personal-data breach occurs, TTA will assess the incident and notify affected individuals or the Information Commissioner where required by law.

15. HOW LONG WE KEEP PERSONAL DATA

We retain personal data only for as long as reasonably necessary for the purpose for which it was obtained, including legal, contractual, insurance, accounting and dispute-related requirements.

15.1 Prospective enquiries

Information concerning an enquiry which does not become an active engagement will normally be retained for up to 12 months after the last substantive communication, unless a longer period is reasonably required.

15.2 Client Matter files

Matter files will normally be retained for six years after the Matter is closed.

A longer period may apply where reasonably necessary because of:

- a) continuing contractual obligations;
- b) litigation or a threatened claim;
- c) a complaint or regulatory investigation;
- d) an outstanding Fee;
- e) an ongoing professional handover;
- f) insurance requirements; or
- g) another lawful reason.

A Matter which is Awaiting Client, Dormant, suspended or subject to a dormant-case retainer may be retained as an open or inactive Matter until it is formally closed.

The six-year Matter-file retention period will ordinarily run from the date of formal closure.

15.3 Call recordings

Call recordings will normally be retained for up to 12 months.

Where a recording:

- a) forms part of the Matter evidence;
- b) records a material instruction;
- c) concerns a complaint;
- d) relates to a disputed agreement or Fee; or
- e) is reasonably required to protect legal rights,

it may be retained with the Matter file for the applicable Matter-file retention period.

15.4 Financial and corporate records

Invoices, payment records and accounting information will be retained for the periods required by applicable tax, accounting and company law.

15.5 Rights requests and complaints

Records of data-protection rights requests and complaints will normally be retained for up to six years after final resolution where reasonably necessary to demonstrate compliance or protect legal rights.

15.6 Marketing information

Marketing information will be retained until the individual opts out or the information is no longer reasonably required.

A minimal suppression record may be retained after an opt-out to ensure that the individual is not contacted again improperly.

At the end of an applicable retention period, personal data will be securely deleted, anonymised or retained only where another lawful reason applies.

16. YOUR DATA-PROTECTION RIGHTS

Depending upon the circumstances, individuals may have the right to:

- a) be informed about how their personal data is used;
- b) request access to their personal data;
- c) request correction of inaccurate or incomplete personal data;
- d) request deletion of personal data;
- e) request restriction of processing;
- f) object to processing based upon legitimate interests;
- g) receive certain personal data in a portable format;
- h) withdraw consent where processing is based upon consent;
- i) request information about automated decision-making; and

j) complain about the handling of their personal data.

These rights are not absolute. A request may be limited or refused where an exemption or other lawful reason applies.

We may request information reasonably required to:

- a) confirm identity;
- b) identify the relevant records;
- c) confirm authority where a request is made for another person; and
- d) protect personal data concerning third parties.

We will respond within the period required by applicable law.

Requests should be sent to:

Email: contact@thetelecomsadvocate.com

Telephone: 02031 431390

Post: The Telecoms Advocate Ltd, 124–128 City Road, London EC1V 2NX

RIGHT TO OBJECT

Where we rely upon legitimate interests to process your personal data, you may have the right to object to that processing on grounds relating to your particular situation.

You have an absolute right to object at any time to the use of your personal data for direct marketing.

To exercise your right to object, please contact us using the details set out below.

17. DATA-PROTECTION COMPLAINTS

A person who is dissatisfied with the way TTA has handled their personal data may make a data-protection complaint by contacting:

James Brookbank

The Telecoms Advocate Ltd

Registered Office: 124–128 City Road, London EC1V 2NX

Email: contact@thetelecomsadvocate.com

Telephone: 02031 431390

ICO Registration Reference: ZC058993

The complaint should, where possible, identify:

- a) the personal data or processing complained about;
- b) what the complainant believes has gone wrong;
- c) relevant dates and communications; and
- d) the outcome sought.

TTA will:

- a) provide a clear means of making a complaint;
- b) acknowledge receipt within 30 days;
- c) make appropriate enquiries without undue delay;
- d) keep the complainant reasonably informed; and
- e) communicate the outcome without undue delay.

These complaint-handling duties have applied since 19 June 2026.

A person also has the right to complain to the Information Commissioner's Office.

The Information Commissioner's Office may be contacted through its official complaints service or by telephone on:

0303 123 1113

A complaint to TTA does not remove or delay the right to contact the Information Commissioner or seek another available remedy.

18. WEBSITE, COOKIES AND ANALYTICS

Our website may use cookies or similar technologies for:

- a) essential website operation;
- b) security;

- c) remembering preferences;
- d) performance monitoring;
- e) analytics; and
- f) other functions described in our Cookie Policy or cookie-management tool.

Where reasonably practicable, analytics information will be anonymised or aggregated.

Where consent is legally required for a non-essential cookie or similar technology, the technology will not be used before valid consent has been obtained.

Users may manage cookie choices through the website's consent controls or browser settings.

Blocking some cookies may affect website functionality.

PECR can apply to cookies and similar technologies whether or not the resulting information is personal data.

19. THIRD-PARTY WEBSITES AND SERVICES

Our website, emails or documents may contain links to third-party websites or services.

TTA is not responsible for the privacy practices of an independent third party.

Individuals should review the privacy information provided by the relevant third party before submitting personal data.

20. CHANGES TO THIS POLICY

We may update this Privacy Policy to reflect:

- a) changes in law or regulatory guidance;
- b) changes to our Services;
- c) changes to our systems or suppliers;
- d) changes to our information-handling practices; or
- e) improvements to clarity and transparency.

The current version of this Privacy Policy will be made available on our website and will identify its effective date.

Where a change materially affects how existing personal data is used, we will take reasonable steps to provide appropriate notice before commencing the new processing where required.

Version 2.4 replaces Version 2.2 from the Effective Date.

21. CONTACTING US

Questions, requests or concerns about this Privacy Policy or TTA's use of personal data should be directed to:

The Telecoms Advocate Ltd

For the attention of: James Brookbank

Registered Office: 124–128 City Road, London EC1V 2NX

Website: www.thetelecomsadvocate.com

Email: contact@thetelecomsadvocate.com

Telephone: 02031 431390

ICO Registration Reference: ZC058993

END OF PRIVACY POLICY