Clicks&Trades Privacy Policy

Last Updated: 18/03/2026

Clicks&Trades College BV

Atealaan 1

2270 Herenthout

Belgium, Europe

BE 1034189452

This Privacy Policy explains how Clicks&Trades College BV ("Clicks&Trades", "we", "our", or "us") collects, uses, stores, discloses, and otherwise processes personal data when you visit our websites, use our digital products, register for courses, webinars, events or newsletters, purchase services, communicate with us, or otherwise interact with us. It also describes your privacy rights and the choices available to you.

This Policy is intended to comply with Regulation (EU) 2016/679 (the General Data Protection Regulation or GDPR), the Belgian Act of 30 July 2018 on the protection of natural persons with regard to the processing of personal data, and other applicable Belgian and EU rules that may apply to online communications, direct marketing, and the use of cookies or similar technologies.

Please read this Policy carefully. By continuing to use our services, you acknowledge that you have been informed about the processing of your personal data as described here. Where consent is required by law, we will request it separately.

1. Data Controller and Contact Details

The controller responsible for the processing of your personal data is Clicks&Trades College BV, Atealaan 1, 2270 Herenthout, Belgium, registered under enterprise number BE 1034189452.

Unless a different contact point is expressly identified for a particular service, privacy-related requests may be sent to the postal address above or to the contact email address published on the relevant Clicks&Trades website or customer communication channel. Where operationally appropriate, we may also route requests internally to the team best placed to respond.

If we appoint a data protection officer or another dedicated privacy contact in the future, the relevant details will be published on our website and, where required, in updated privacy notices.

2. Scope of This Policy

This Policy applies to personal data processed in connection with our websites, landing pages, online forms, educational portals, software tools, customer support channels, newsletters, social media pages, online communities, in-person and online events, and any services, products, or content that link to or reference this Policy.

This Policy applies whether you interact with us as a visitor, subscriber, student, customer, lead, event attendee, supplier contact, business partner contact, job applicant, or another individual whose personal data we receive in the course of operating our business.

This Policy does not apply to third-party websites, platforms, brokers, exchanges, payment providers, social networks, app stores, or other services that we do not control, even if our services contain links to them. Those third parties remain responsible for their own privacy practices, and you should review their privacy notices separately.

3. Definitions

"Personal Data" means any information relating to an identified or identifiable natural person, including direct identifiers such as a name or email address and indirect identifiers such as an IP address, cookie identifier, device identifier, or information linked to a person.

"Processing" means any operation performed on personal data, including collection, recording, organisation, storage, consultation, use, disclosure, combination, restriction, deletion, or destruction.

"Data Subject" means the individual to whom the personal data relates.

"Controller" means the person or organisation that determines the purposes and means of the processing of personal data.

"Processor" means a person or organisation that processes personal data on behalf of a controller under appropriate contractual safeguards.

"Services" means our websites, educational offers, newsletters, digital products, events, support activities, and related commercial or informational services.

"Website" means any Clicks&Trades-operated website, landing page, portal, or microsite that links to this Policy.

"GDPR" means Regulation (EU) 2016/679 as amended, supplemented, or replaced from time to time.

4. Categories of Personal Data We Collect

We collect personal data directly from you, automatically from your use of our services, and in some cases from third parties such as analytics providers, payment providers, advertising partners, social networks, event tools, public sources, or service providers acting on our behalf. The categories of data we may process include the following:

Category	Examples of Personal Data
Identity and contact data	Name, email address, postal address, telephone number, business name, title, billing or delivery contact details.
Account and profile data	Login credentials, username, password hash, account preferences, saved settings, course enrolment details, student profile information, membership status.
Transaction and billing data	Order details, invoices, payment status, payment method metadata, VAT-related details, refund or chargeback information. Full payment card data is typically processed by our payment service providers rather than stored by us.

Course, event, and service data	Programmes purchased, attendance records, certificates, webinar participation, event registration data, assignments submitted, progress tracking, feedback, survey responses, and support history.
Communication data	Emails, chat messages, support requests, call notes, meeting notes, social media messages, form submissions, and other content you send to us.
Technical and usage data	IP address, browser type, operating system, device identifiers, language settings, pages visited, clickstream data, session information, referring URLs, approximate geolocation inferred from IP, crash logs, and diagnostics.
Marketing and preference data	Newsletter sign-up information, subscription preferences, campaign responses, lead source, advertising interactions, cookie choices, and suppression lists used to respect opt-out requests.
Media and content data	Images, audio, video, testimonials, comments, posts, uploaded files, and other content you choose to provide, including when participating in community spaces or events.
Compliance and risk data	Records needed to comply with legal obligations, fraud prevention, security monitoring, complaints handling, dispute management, or regulatory inquiries.
Public and third-party data	Public social media profile information, publicly available business details, partner-provided lead information, analytics data, and other information lawfully shared with us by third parties.

We do not intentionally request special categories of personal data, such as information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data used for the purpose of uniquely identifying a person, health data, or data concerning sex life or sexual orientation, unless this is strictly necessary for a specific lawful purpose and appropriate safeguards are in place. If you voluntarily provide such information, please avoid sharing more than is necessary.

5. Sources of Personal Data

- Directly from you when you complete forms, create an account, subscribe to newsletters, request information, purchase products or services, attend events, join programmes, communicate with us, or otherwise interact with us.
- Automatically when you browse our websites or use our services, through server logs, cookies, pixels, SDKs, local storage, analytics tools, and similar technologies.
- From third parties such as payment providers, analytics services, advertising networks, CRM tools, event platforms, social media networks, affiliate partners, resellers, hosting providers, public registers, and publicly available online sources, where those parties are permitted to share data with us.

- From business partners, employers, team leaders, or referral contacts where they lawfully provide your details to register you for a programme, invite you to an event, or otherwise coordinate a legitimate business interaction with us.

6. Purposes of Processing and Legal Bases

We only process personal data when a valid legal basis exists under Article 6 GDPR or another applicable legal rule. Depending on the circumstances, one or more of the following legal bases may apply: consent, performance of a contract, compliance with a legal obligation, protection of vital interests, public interest where applicable, and our legitimate interests, provided those interests are not overridden by your fundamental rights and freedoms.

Purpose	Legal Basis	Examples
To provide requested services and administer your relationship with us	Performance of a contract; legitimate interests	Creating accounts, enrolling you in courses or communities, delivering newsletters or digital content you requested, providing support, processing renewals, issuing invoices, and managing attendance or certifications.
To process payments and manage accounting obligations	Performance of a contract; legal obligation	Billing, VAT administration, bookkeeping, refunds, debt collection, and financial record retention.
To communicate with you	Performance of a contract; legitimate interests; consent in some cases	Sending service messages, responding to inquiries, confirming registrations, providing support, sharing updates about events, and managing operational notifications.
To improve and secure our services	Legitimate interests; legal obligation in some cases	Monitoring usage, preventing abuse, maintaining platform integrity, troubleshooting bugs, detecting fraud, and enforcing our terms or internal policies.
To send direct marketing	Consent where required; legitimate interests where permitted by law	Sending newsletters, updates, educational content, promotions, and relevant offers by email, SMS, social media, or other electronic means in accordance with applicable rules.
To personalise content and measure campaigns	Consent where required for cookies or similar technologies; legitimate interests where lawful	Understanding audience engagement, measuring campaign effectiveness, tailoring content, and improving conversion pathways.
To comply with legal and regulatory obligations	Legal obligation	Responding to lawful requests, preserving records, handling complaints, defending claims, and complying with tax, accounting, consumer, or data protection rules.
To protect our rights and business	Legitimate interests	Corporate structuring, due diligence,

interests		audits, insurance, dispute resolution, internal reporting, and business continuity planning.
To recruit and evaluate applicants	Pre-contractual steps; legitimate interests; legal obligation where applicable	Assessing applications, scheduling interviews, verifying background information where lawful, and keeping records required for HR administration.

Where we rely on legitimate interests, we consider the nature of the data, the context of the processing, the reasonable expectations of the individuals involved, and the safeguards we can apply to reduce privacy impact. You may object to processing based on legitimate interests in the circumstances described in this Policy and the GDPR.

Where we rely on consent, you may withdraw that consent at any time. Withdrawal will not affect the lawfulness of processing carried out before the withdrawal.

7. Cookies, Similar Technologies, and Online Tracking

Our websites and digital services may use cookies, local storage, pixels, tags, SDKs, scripts, and similar technologies to make the website function, remember preferences, secure sessions, analyse traffic, measure campaign performance, and, where permitted, personalise content or advertisements.

Some technologies are strictly necessary for the operation and security of the website and do not require consent under applicable rules. Other technologies, including certain analytics, personalisation, and advertising cookies, will only be placed or activated after you have given consent where such consent is legally required.

You can manage your preferences through our cookie banner or preference centre where available, and you can also adjust your browser settings to refuse or delete cookies. Please note that disabling certain cookies may affect the availability, functionality, or performance of parts of our services.

Where a separate Cookie Policy or Cookie Notice is published on a specific Clicks&Trades website, that document supplements this Privacy Policy and provides more detailed information on the categories of cookies used, the purposes, retention periods, and third parties involved.

8. Direct Marketing and Communications Preferences

We may send you service-related communications that are necessary for the performance of our contract with you or for our legitimate interests in operating our business. These communications may include account notices, purchase confirmations, event reminders, billing information, security notices, and essential updates relating to products or services you use.

We may also send direct marketing communications about our courses, products, services, events, educational materials, special offers, and related business opportunities. Where required by law, we will do so only with your prior consent. In other cases, we may rely on a lawful exception or our legitimate interests where this is permitted under applicable law and where you are always given a clear opportunity to opt out.

You may unsubscribe from marketing emails by using the unsubscribe link included in the message, by changing your account preferences where available, or by contacting us. We may retain limited

information, such as your email address and opt-out status, in order to honour your request and maintain suppression lists.

9. Sharing of Personal Data

We do not sell your personal data in the ordinary sense of transferring ownership of customer lists for money. However, we may share personal data with carefully selected recipients where this is necessary for the purposes described in this Policy or where we are legally required or permitted to do so. Recipients may include:

- Service providers and processors that help us host websites, manage customer relationships, deliver email and messaging services, process payments, provide analytics, run webinars and events, store documents, support learning platforms, prevent fraud, maintain security, or otherwise support our operations.
- Professional advisers such as lawyers, accountants, auditors, insurers, financial advisers, and compliance consultants who need access to information in the course of advising us or protecting our legal interests.
- Business partners, resellers, affiliates, instructors, or event co-organisers where sharing is necessary to deliver a joint offering, coordinate attendance, attribute referrals, administer an offer, or provide the service you requested.
- Public authorities, regulators, courts, tax authorities, law enforcement agencies, or other third parties where disclosure is required by law, judicial order, legal process, or where necessary to protect rights, safety, and security.
- Potential buyers, investors, lenders, insurers, and transaction advisers in connection with an actual or proposed merger, acquisition, reorganisation, financing, sale of assets, or other corporate transaction, subject to appropriate confidentiality safeguards.
- Other parties with your consent or at your direction, for example when you ask us to share information with a third-party service or business contact.

Where another party processes personal data on our behalf as a processor, we seek to put in place contracts required by Article 28 GDPR or equivalent contractual safeguards. These contracts generally require processors to act only on documented instructions, maintain confidentiality, implement appropriate security measures, and assist us with our data protection obligations.

10. International Transfers

Some of our service providers, technical systems, partners, or support resources may be located outside Belgium or the European Economic Area, or may access personal data from outside the EEA. When personal data is transferred to a country that has not been recognised by the European Commission as providing an adequate level of protection, we seek to implement an appropriate safeguard under Chapter V GDPR.

Depending on the circumstances, these safeguards may include an adequacy decision, the European Commission’s Standard Contractual Clauses, supplementary technical and organisational measures, Binding Corporate Rules, an approved code of conduct, an approved certification mechanism, or another lawful transfer mechanism permitted by the GDPR.

You may request additional information about the relevant transfer safeguards that apply to your personal data, subject to the protection of confidential business information and legal limitations.

11. Data Retention

We keep personal data only for as long as necessary for the purpose for which it was collected, or for longer where this is required or permitted by law. Retention periods can vary depending on the nature of the service, the sensitivity of the information, the legal basis for the processing, and our need to resolve disputes, enforce agreements, comply with statutory recordkeeping obligations, or defend legal claims.

When determining retention periods, we take into account the volume, nature, and sensitivity of the data; the potential risk of harm from unauthorised use or disclosure; whether the purposes can be achieved through other means; and the applicable legal, tax, accounting, contractual, and regulatory requirements.

- Account, contract, and transaction records are generally retained for the duration of the contractual relationship and for a reasonable period thereafter to address complaints, audits, accounting obligations, and potential legal claims.
- Marketing contact data is typically retained until you unsubscribe, object, withdraw consent, or until the data becomes inactive and is no longer needed for the relevant campaign or relationship-management purpose.
- Support requests, security logs, and technical records may be retained for shorter operational periods or longer where necessary for fraud prevention, system integrity, and legal compliance.
- Cookie-related retention periods vary depending on the cookie type and are described in more detail in the relevant cookie notice where published.

When personal data is no longer required, we will delete it, anonymise it, or securely isolate it from routine use, unless continued storage is required by law or necessary to establish, exercise, or defend legal claims.

12. Security of Personal Data

We implement appropriate technical and organisational measures designed to protect personal data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure, and unauthorised access. The measures we use depend on the nature of the data and the processing risks and may include access controls, role-based permissions, password and authentication measures, logging, encryption in transit where appropriate, secure backups, vendor due diligence, staff confidentiality obligations, and internal policies governing data handling.

No method of transmission over the internet and no electronic storage system is completely secure. For that reason, although we take reasonable and proportionate steps to protect information, we cannot guarantee absolute security. You should also take steps to protect your own devices, passwords, and accounts and notify us promptly if you suspect misuse of your account or a security issue affecting your interaction with us.

If we become aware of a personal data breach, we will assess the incident and take the measures required by applicable law, including notification to the competent supervisory authority and affected individuals where legally required.

13. Your Rights Under the GDPR

Subject to the conditions and limitations set out in applicable law, you may have the following rights in relation to your personal data:

- Right of access: to obtain confirmation of whether we process your personal data and, if so, to receive access to that data and related information.
- Right to rectification: to ask us to correct inaccurate personal data or complete incomplete data.
- Right to erasure: to request deletion of personal data in certain circumstances, for example where the data is no longer necessary or where consent is withdrawn and no other legal basis applies.
- Right to restriction: to request that we limit processing in certain situations, for example while a dispute about accuracy or legal basis is being resolved.
- Right to data portability: to receive certain personal data you provided to us in a structured, commonly used, and machine-readable format, and to transmit that data to another controller where technically feasible.
- Right to object: to object, on grounds relating to your particular situation, to processing based on legitimate interests, and to object at any time to processing for direct marketing purposes.
- Right not to be subject to certain automated decision-making: to request human review where a decision producing legal or similarly significant effects is based solely on automated processing, where applicable.
- Right to withdraw consent: where processing is based on consent, to withdraw that consent at any time without affecting prior lawful processing.
- Right to lodge a complaint: to submit a complaint to the Belgian Data Protection Authority or another competent supervisory authority if you believe your rights have been infringed.

To exercise your rights, please contact us using the details set out in this Policy. We may ask you for additional information to verify your identity before responding. This helps us protect personal data against unauthorised disclosure. We will respond within the period required by applicable law, subject to any lawful extensions.

In some cases, we may refuse or limit a request where the GDPR permits us to do so, for example where the request is manifestly unfounded or excessive, where disclosure would adversely affect the rights of others, or where we must retain certain data to comply with legal obligations or defend claims.

14. Complaints and Supervisory Authority

If you have concerns about how we handle your personal data, we encourage you to contact us first so that we can try to resolve the issue. You also have the right to lodge a complaint with the Belgian Data Protection Authority (Gegevensbeschermingsautoriteit / Autorité de protection des données), Drukpersstraat 35, 1000 Brussels, Belgium.

You may also have the right to seek a judicial remedy or to lodge a complaint with the supervisory authority in the EU Member State of your habitual residence, place of work, or place of the alleged infringement, as provided by the GDPR.

15. Children and Minors

Our services are generally intended for adults, business users, and individuals who can validly enter into agreements or provide consent under applicable law. We do not knowingly collect personal data

directly from children where such collection would require parental consent and that consent has not been obtained.

If a course, event, educational programme, or community is specifically offered to minors, additional information may be provided at the point of collection and parental or guardian consent may be requested where required by law. If you believe that a child has provided personal data to us inappropriately, please contact us so that we can take appropriate steps.

16. Social Media, Communities, and User-Generated Content

If you interact with us on social media or in public or semi-public community spaces, the information you submit may be visible to other users, the platform provider, and the public, depending on the settings of the service involved. Please avoid posting personal data that you do not want others to see or re-use.

When we operate pages or communities on third-party platforms, we and the platform provider may each have responsibilities for certain processing activities. The platform remains responsible for its own infrastructure, cookies, profiling, and platform analytics. You should review the privacy information supplied by the relevant provider for more detail.

If you give us permission to publish testimonials, reviews, quotes, photographs, recordings, or success stories, we may use that content for promotional or educational purposes in accordance with the permission granted and any applicable legal requirements. You may contact us if you later wish to withdraw the permission, although continued use may still be lawful where another legal basis applies or where removal is not reasonably possible in archived material already distributed.

17. Events, Courses, and Educational Services

Because Clicks&Trades operates educational and training-related services, we may process additional data in the context of enrolment, attendance, participation, progress monitoring, assignments, coaching, webinars, workshops, community management, and certification. This may include learning preferences, participation history, event sign-in records, submitted coursework, Q&A logs, and feedback provided by you or, where relevant, by an employer or sponsor that enrolled you.

We use this information to administer programmes, verify attendance, improve our educational offerings, issue completion records where applicable, manage scheduling and event logistics, and provide customer service. Depending on the context, this processing may be necessary for performance of a contract, our legitimate interests in operating and improving our services, or compliance with legal obligations.

Where sessions are recorded, photographs are taken, or screenshots are captured during an event, webinar, workshop, or community session, we will provide notice as appropriate. Recordings may be used for replay access, internal quality review, educational archives, security purposes, or promotional activities where a lawful basis exists. If a recording is optional and your participation is not essential to the recording purpose, we may offer practical alternatives where appropriate, such as asking participants to keep cameras off or to submit questions through chat.

18. Payments, Finance, and Anti-Fraud Controls

If you purchase a service from us, payment processing is generally handled by specialised third-party payment providers. We receive transaction confirmations and limited payment-related metadata necessary to fulfil the order, manage billing, prevent fraud, support customer service, and maintain financial records. We do not ordinarily store full payment card numbers or security codes on our own systems unless a payment method designed for secure tokenised storage expressly requires it and is lawfully implemented.

We may process data needed to detect and prevent fraud, misuse, chargebacks, unauthorised transactions, and other forms of abuse. This may involve risk scoring, order verification, device or IP checks, log analysis, and sharing limited information with payment providers or relevant authorities where justified.

19. Recruitment and Business Contact Information

If you apply for a role with us or otherwise send us professional information in a recruitment context, we may process your CV, application documents, interview notes, references, publicly available professional profile information, and communications relating to the vacancy. We use this data to assess your suitability, communicate with you, and manage the recruitment process. Unless a longer period is justified and lawful, recruitment data is retained only for as long as reasonably necessary to complete the process and address follow-up issues.

We may also process personal data relating to suppliers, contractors, instructors, introducers, affiliates, or representatives of business customers and partners. This is usually limited to business contact details and relationship-management information and is processed for contract administration, service coordination, compliance, accounting, and legitimate business operations.

20. Automated Decision-Making and Profiling

We may use limited forms of automation to segment audiences, personalise communications, detect abuse, score engagement, or prioritise support and operational tasks. However, we do not normally make decisions based solely on automated processing that produce legal effects or similarly significant effects on individuals without appropriate safeguards.

If a service were to involve such automated decision-making in the future, we would provide additional information as required by law, including meaningful information about the logic involved and the significance and envisaged consequences of the processing for the individual concerned.

21. Data Minimisation and Accuracy

We aim to collect only the personal data that is relevant and reasonably necessary for the purposes described in this Policy. We also take reasonable steps to keep personal data accurate and up to date. You can help us by informing us promptly of changes to your contact details or other relevant information.

If you provide personal data relating to another person, you are responsible for ensuring that you have the right to do so and, where required, that you have informed that person about the content of this Policy.

22. Legal Claims, Corporate Transactions, and Reorganisation

We may preserve, review, and disclose personal data where necessary to establish, exercise, or defend legal claims, to enforce our agreements, to investigate complaints or disputes, or to protect our company, our users, our staff, and third parties. This may include sharing data with insurers, advisers, counterparties, courts, or competent authorities.

If our business is sold, merged, reorganised, financed, or transferred in whole or in part, personal data may be transferred to relevant counterparties and advisers subject to confidentiality obligations and lawful safeguards. In such cases, we will take reasonable steps to ensure continuity of protection for the personal data involved.

23. Updates to This Policy

We may update this Privacy Policy from time to time to reflect legal, technical, or business developments. When we do, we will publish the updated version on the relevant website and amend the "Last Updated" date at the top of the Policy. If the changes are material, we may also provide additional notice through email, platform notifications, or other appropriate communication channels.

Your continued use of our services after an updated Policy becomes effective means that you have been informed of the revised terms, to the extent permitted by law. Where a change requires fresh consent, we will seek that consent separately.

24. Contacting Us About Privacy

If you have questions, requests, or complaints regarding this Privacy Policy or our processing of personal data, you may contact Clicks&Trades College BV at Atealaan 1, 2270 Herenthout, Belgium. You may also use the support or contact email address published on the applicable Clicks&Trades website or service through which you interact with us.

To help us process your request efficiently, please describe the nature of your request and the context in which you interacted with us. Where necessary, we may request information to verify your identity before disclosing or modifying personal data.

25. Final Provisions

This Privacy Policy is intended to provide a clear and comprehensive explanation of our privacy practices. If any part of this Policy is found to be invalid or unenforceable, the remaining provisions will continue in effect to the fullest extent permitted by law. This Policy shall be interpreted in a manner consistent with applicable Belgian and EU data protection law.

Nothing in this Policy is intended to limit any rights you may have under mandatory law or any obligations that we may have under mandatory law. In the event of inconsistency between this Policy and mandatory legal requirements, the applicable legal requirements will prevail.

Appendix 1. Indicative Retention Schedule

The following retention schedule is indicative and may be adjusted where a longer or shorter period is justified by the nature of the service, a legal obligation, an unresolved dispute, a regulatory inquiry, or another documented business need. Where multiple retention periods could apply to the same data set, the longest lawful and relevant period may govern.

Record Type	Indicative Retention Approach
Website server logs and security logs	Generally short-term operational retention; may be retained longer if needed for incident investigation, abuse prevention, or evidentiary preservation.
Customer account records	For the active life of the account and a reasonable period thereafter to manage support, disputes, and legal obligations.
Invoices and accounting records	For the period required by tax, accounting, and statutory recordkeeping obligations under applicable law.
Support correspondence	For as long as needed to address the issue raised, maintain service continuity, train staff, or defend claims.
Marketing subscriber lists	Until consent is withdrawn, objection is received, or the contact becomes inactive and no longer relevant for the intended purpose.
Suppression and opt-out records	For as long as necessary to ensure future marketing preferences are respected.
Webinar and event registration data	For programme administration and a reasonable follow-up period, unless longer retention is justified for compliance, certification, or dispute handling.
Recorded sessions	For the period communicated at the time of recording or for as long as needed for replay access, educational archives, and quality review, subject to applicable law.
Recruitment materials	For the duration of the recruitment process and, where lawful, a limited additional retention period for future opportunities or legal compliance.
Contract files and due diligence records	For the life of the contract and any follow-up period needed for audit, limitation periods, and business continuity.

Appendix 2. How We Handle Data Subject Requests

When we receive a privacy request, we may first review the request to determine its scope, whether we hold data that falls within the request, and whether additional identity verification is needed. Where the request is broad or unclear, we may ask you to clarify the specific service, date range, email address, or other details that will help us locate the relevant information more efficiently.

We aim to respond without undue delay and within the time frame required by the GDPR. If a request is complex or numerous, the response period may be extended where the law allows. In that case, we will inform you of the extension and the reasons for it.

In certain situations, we may need to balance your request against the rights and freedoms of others, our trade secrets and confidential business information, the integrity of our systems, or our obligations to preserve data for legal, accounting, fraud-prevention, or regulatory reasons. Where we cannot fully comply with a request, we will explain the basis for our position to the extent permitted by law.

If you request access to specific communications, recordings, assignments, certificates, or transactional records, we may provide the information through a secure channel, by allowing account access, by sending copies, or by explaining why certain categories are not available or no longer retained.

Appendix 3. Practical Privacy Principles Applied by Clicks&Trades

- Transparency: we aim to explain our processing activities in clear language through this Policy, just-in-time notices, contract terms, and cookie controls where relevant.
- Purpose limitation: we seek to use personal data only for specified, explicit, and legitimate purposes and to avoid incompatible re-use unless another legal basis or notice applies.
- Data minimisation: we aim to collect the least amount of personal data reasonably necessary for the service or business need involved.
- Accuracy: we take reasonable steps to keep records current and invite users to update their information when changes occur.
- Storage limitation: we do not keep personal data forever by default and use retention criteria to support deletion, anonymisation, or restricted storage.
- Integrity and confidentiality: we use appropriate technical and organisational safeguards, vendor controls, and internal access restrictions designed to protect personal data.
- Accountability: we maintain internal governance processes and review our practices over time to support ongoing compliance.