Data processing annex (English courtesy translation)

Version 8.3, courtesy translation of the French version, annex to the WhoHeld Terms of Service. Only the French version is binding: in case of divergence, the French version prevails (article 15.6 of the Terms of Service).

Between the **Client** identified in the Order Form **and WhoHeld**, société par actions simplifiée unipersonnelle, 49 cours Mirabeau, 13100 Aix-en-Provence, France, Trade and Companies Register (RCS) Aix-en-Provence 130 164 783 (hereinafter "**the Publisher**").

This annex forms an integral part of the Contract and **prevails** over the Terms of Service in the event of contradiction regarding the processing of personal data.

The Publisher's compliance documentation (qualification, balancing test, retention periods, impact assessment, due diligence on the source, security measures) is set out in a **Compliance Note**, provided on request under a confidentiality agreement. It is not contractual.

Preamble: two regimes

The Publisher requests no access to the Client's Seller Central or Vendor Central account and receives no data from it: collection is carried out from outside. This results in two distinct regimes.

	Subject matter	Capacity of the Publisher
A	Market data and data on third-party sellers	**Controller**, on its own account
B	User accounts, security, invoicing	**Processor** for the administration of accounts; **separate controller** for security, logging and usage measurement

---

Part I. What the Publisher does not process

The Publisher **does not collect and does not receive**: data from the Client's merchant account; data on buyers or end consumers (identities, delivery addresses, contact details, purchase histories, order contents); payment data of their customers; special categories of data within the meaning of article 9, or data relating to criminal convictions (article 10).

The Client shall not enter such data into the Platform; its configuration (declared catalogue, tracked categories, roles assigned to sellers) contains none. **This commitment is contractual**: any change to

the product leading the Publisher to process buyer data would be the subject of an amendment including a processing agreement compliant with article 28.

Part II. Regime A: market data and data on third-party sellers

A.1 Capacity of the Publisher

The Publisher is a controller within the meaning of article 4(7) of the GDPR. The Parties acknowledge that it alone determines the sources, the frequency of observation, the calculation methods and the retention periods; that collection is pooled between its clients; that the observation base pre-exists the start of the relationship with a Client and survives it; that it alone is responsible for informing data subjects and handling their requests; and that the Client has access neither to the means of collection, nor to the sources, nor to the data as acquired, but to analysis Results that it may export.

The Client's selection of its scope, and the roles it assigns to the sellers it observes, are exercised among pre-existing possibilities and **relate only to what is reported to it**: they have no effect on the sources, methods, retention periods or purposes of the processing, which the Publisher alone determines. The Client's declaration of its own catalogue references may lead the Publisher to observe references that were not yet observed; **this declaration designates objects to be observed within a processing operation of which the Publisher alone determines all the means (source, fields, methods, actual frequency, retention periods) and all the purposes**; the Parties consider that it does not constitute a joint determination of the purposes and means within the meaning of article 26, subject to the qualification resulting from the factual circumstances, article A.2 applying if joint controllership were found. **The "committed collection frequency" set by the Order Form (articles 1.1 and 4 of the Terms of Service) is a commercial service level (the minimum number of observations guaranteed to the Client for its Scope) and not an instruction from the Client on the means of collection**: it, too, relates only to what is reported to the Client, never to the method, the actual schedule or the pooling of collection between Clients.

A.2 Fallback clause

The qualification results from the factual circumstances, not from the will of the Parties alone. **If a supervisory authority or a court were to find joint controllership, this article constitutes an arrangement within the meaning of article 26(1)**: the **Publisher** is responsible for informing data subjects (articles 13 and 14), for all requests to exercise rights (articles 15 to 22), for security (article 32), for documentation, for notification of breaches (articles 33 and 34) and for the impact assessment (article 35); the **Client** is responsible for the lawfulness of the use it makes of the Results and for the deletion provided for in article A.4. In such a case, the Publisher makes the essence of this arrangement available to data subjects in the notice published at https://whoheld.com/trust/sellers-notice (article 26(2)). The Publisher remains the contact point for data subjects, without prejudice to article 26(3).

A.3 Legal basis, information, retention periods

The processing is based on **legitimate interest** (article 6(1)(f)), following a three-step balancing test set out in the Compliance Note.

As the data are collected indirectly, the Publisher publishes and maintains at https://whoheld.com/trust/sellers-notice, **from October 1, 2026**, a **free and freely accessible notice** containing all the information required by articles 14(1) and 14(2), including the source, **the retention periods** and **the right to object**, in French, English, German, Spanish and Italian, the English version also being addressed to sellers on marketplaces located outside Europe. The retention periods applied are those published in that notice and in the Privacy Policy.

The processing involves **profiling** (article 4(4)) limited to the selling activity carried out towards the public. **No Result is designed to constitute, on its own or in a determining way, the basis of a decision producing legal effects concerning a seller who is a natural person or similarly significantly affecting them** (article 22, as interpreted by the CJEU in the *SCHUFA* judgment, C-634/21); the Platform executes no automated decision, and the Client shall not use a Result as the exclusive or determining basis of such a decision without a prior compliance analysis.

A.4 Sellers' rights

The Publisher handles sellers' requests directly, without involvement of the Client. **The objection is exercised free of charge and with no condition other than the statement of grounds relating to the person's particular situation** (article 21(1)); at the person's request, the processing is restricted during the examination (article 18(1)(d)). The Publisher continues only if it **demonstrates** compelling legitimate grounds which override the person's rights, or the necessity of the processing for the establishment, exercise or defence of legal claims. Otherwise, it stops the processing, erases the nominative data, prevents their reintroduction in subsequent collections and **notifies the erasure to each of its recipients** (article 19), that is to say to its clients, the only recipients to which it reports Results; erasure at its hosting processors results from the deletion in the database, and authorities seized by way of a lawful request are not recipients for the purposes of this notification. Mentions of the seller's name in the questions asked by Users to Ask WhoHeld and in the answers kept in that assistant's log are not covered by this erasure: they are deleted no later than twelve (12) months after they are recorded, by the purge of that log.

Client's obligation. The Client does not handle any seller request: it forwards it to the Publisher without replying to it. Upon written notification from the Publisher identifying the seller concerned, the Client stops using the seller's name in its reporting and deletes the corresponding nominative data **from the active and structured systems in which it exploits them**, within **sixty (60) days**.

Relay to its own recipients. Article 3.3 of the Terms of Service authorises the Client to disclose Results to the companies of its group, to its advisers, to its e-commerce agencies and service providers and to its contacts within the marketplaces, in the form of processed Results, never the raw data or anything from which they could be reconstructed, and under equivalent confidentiality. **The Publisher does not know these recipients**: its notification stops at its own recipients. Where it has disclosed the Results concerned, **the Client relays the information to those of its recipients to which it has transmitted them**, within the same period, where that relay is reasonably possible in view of the records available to it **and insofar as the Results concerned still allow the seller to be identified**. A Result that is aggregated, anonymised or incorporated into a summary that no longer allows such identification requires no relay.

Limits common to the two preceding obligations. They extend neither to backups, archives and logs subject to an automatic purge cycle, nor to documents already circulated internally, nor to exports more than twenty-four (24) months old; they end thirty-six (36) months after the end of the Contract.

A.5 Consequence for the Client

The Publisher is responsible for documenting the observation base: the record of processing activities, the balancing test, the impact assessment, informing data subjects and handling their requests. Subject only to article A.4, it expects nothing from the Client in this respect: the Client receives an analysis result, not a delegated processing operation. **The Client remains free to document in its own record of processing activities the internal use it makes of the Results**, where they include data relating to sellers who are natural persons, and assesses its obligations under article 24 of the GDPR.

Part III. Regime B: User accounts, security and invoicing

The Publisher is **processor** (article 28) for the creation, management and deletion of User accounts, the allocation of rights, authentication, support and the sending of requested alerts. It is **separate controller**, on the basis of its legitimate interest (article 6(1)(f)) and, for invoicing, of its legal and contractual obligations, for the security of the service, logging and the retention of logs, the investigation of incidents, the usage measurement necessary for invoicing, for monitoring compliance with article 4 of the Terms of Service and for managing the support provided to the Client (pages viewed, aggregated per client account), the production of aggregated and anonymised statistics, and **support for the free evaluation** (Terms of Service 1.5: exchanges with Users, usage indicators during the evaluation, series of onboarding messages, proof of acceptance of the conditions of the evaluation). The Client **informs its Users** of this second capacity (article 13), by reference to the Publisher's Privacy Policy.

B.1 Description of the processing carried out as processor (article 28(3))

Subject matter	Creation, management and securing of the accesses of the Users designated by the Client
Nature	Hosting, authentication, allocation of rights, support
Purpose	Enabling the Client's Users to access the Platform
Duration	Term of the Contract, then the reversibility window of article 12 of the Terms of Service
Data subjects	Employees of the Client and service providers acting solely for the Client's needs, to the exclusion of agencies serving other clients, designated as Users
Data	Surname, first name, professional email address, company, role and rights; product references viewed via the extension, solely for display purposes and without logging

Technical identifiers, IP addresses, login timestamps and activity logs fall under the security processing, for which the Publisher is controller.

B.2 Obligations of the Publisher as processor

a) Process the data **on documented instructions** from the Client (the Contract, this annex and the configuration constitute instructions), and inform the Client immediately if, in its opinion, an instruction infringes the GDPR. **b)** Ensure **confidentiality**: authorised persons are bound by a contractual or statutory obligation. **c)** Implement and maintain the **technical and organisational measures** described in the **Security annex** below (article 32), and update them in line with the state of the art. **d)** Comply with the conditions for **engaging sub-processors** of article C.1. **e) Assist the Client** with requests to exercise rights (removal of a User is available in the Platform to the Client's administrator, except during the free evaluation, or upon written request to the Publisher: the removed account is blocked immediately, its sessions are revoked, then it is deleted within thirty (30) days; export and rectification of an account's data are carried out on request), with security, with the notification of breaches and, where applicable, with the impact assessment (articles 32 to 36); forward to the Client any request received directly **without replying to it**. **f) Notify any personal data breach** to the Client without undue delay and, in any event, **within forty-eight (48) hours** of becoming aware of it, in writing and in a datable manner, specifying the nature of the breach, the categories and approximate number of data subjects and records, the likely consequences, the measures taken and the contact point; preliminary information is sent as soon as the Publisher becomes aware of the event, even if incomplete. **g) Make available the documentation** necessary to demonstrate compliance with article 28 and to allow the audit provided for in article C.3. **h) Keep the record** of the categories of activities carried out on behalf of the Client (article 30(2)). **i) Not use these data for its own purposes**, subject to the processing for which it is controller under this regime and to aggregated and anonymised statistics within the meaning of recital 26: no individualisable person, no correlatable record, no inferable information.

B.3 Fate of the data at the end of the Contract

Reversibility under article 12 of the Terms of Service: read and export access maintained for thirty (30) days, full export on request within fifteen (15) business days, deletion from the production environments within the following thirty (30) days, then from the backups according to a rotation cycle not exceeding ninety (90) days. **Written certificate of deletion** provided on request. Only the data necessary to comply with a legal obligation are kept, for the prescribed period and under the same security regime.

Part IV. Common provisions

C.1 Sub-processors

The Client authorises the sub-processors listed in Annex 1. The Publisher informs the Client of any addition or replacement **at least thirty (30) days** before it is implemented; the Client may object within fifteen (15) days on reasonable grounds relating to data protection; failing agreement within thirty (30) days, it may terminate without compensation, with a refund pro rata temporis. The Publisher imposes on each sub-processor obligations at least equivalent and **remains fully liable to the Client**.

C.2 Location and transfers

The data are hosted **within the European Union** (Annex 1). The sub-processors established outside the Union, Supabase Pte. Ltd. (Singapore), Resend, Vercel Inc. and Functional Software, Inc. (Sentry) (United States), may access them from those countries. Anthropic Ireland, Limited, established in Ireland, has the

data processed in the United States by its parent company, Anthropic, PBC. Anthropic receives pseudonymised data derived from the Results and, where applicable, the data that the User freely types into his or her question to Ask WhoHeld; this flow constitutes a transfer of personal data to the United States; the data are kept for thirty (30) days by Anthropic and then deleted, and are not used to train any model. These transfers are governed by the standard contractual clauses of Commission Implementing Decision (EU) 2021/914, incorporated into their processing agreements. Google Cloud France SARL, 8 rue de Londres, 75009 Paris (Google Workspace), established in the Union, does not allow the region where the data are stored to be chosen in the plan subscribed: email exchanges may be processed in Google data centres located outside the Union, these transfers being governed by the Google Cloud data processing addendum (standard contractual clauses of Implementing Decision (EU) 2021/914; Google LLC is certified under the EU-US Data Privacy Framework). Any other transfer to a third country is subject to an adequacy decision in force on the date of the transfer or, failing that, to the standard contractual clauses of Implementing Decision (EU) 2021/914, together with a transfer impact assessment and appropriate supplementary measures.

Marketplaces outside the Union. The observation of sellers present on marketplaces located outside the Union (United Kingdom, United States, Canada, Japan, Mexico, Brazil, India) **does not constitute a transfer outside the Union**: the data are collected into the Union and hosted there. An outgoing transfer to a provider established in the United Kingdom would be subject to the adequacy decision in force or, failing that, to the standard clauses together with the UK addendum.

C.3 Audit

The Client may verify compliance with Part III **once per twelve (12) month period**, subject to **sixty (60) days'** written notice, by means of the provision of the **compliance file**: Compliance Note, certifications and reports of the infrastructure sub-processors, answers to a security questionnaire. If these elements are insufficient in view of a risk that is **specific and identified in writing**, a documentary audit is conducted **remotely**, by an independent third party appointed by the Client, which is not a competitor and is bound by confidentiality, **within the limit of one (1) day**. An on-site audit takes place only if required by a supervisory authority.

The audit may not cover the data of other clients. It is at the Client's expense, **including the time the Publisher devotes to it beyond one day per twelve-month period**, invoiced at the current rate, unless it reveals a substantial breach. A higher frequency is permitted at the request of an authority or after a proven breach. Regime A is not subject to audit by the Client, the Publisher acting on its own account, **except where article A.2 applies**, in which case the Client may obtain the information necessary for its own obligations under article 26.

C.4 Liability

The respective liability of the Parties is governed by article 82 of the GDPR. In accordance with article 13.3 of the Terms of Service, **the contractual liability cap is not enforceable** against compensation due on that basis.

C.5 Contacts

	Client	**Publisher**
Data protection contact	*(to be completed in the Order Form)*	privacy@whoheld.com

C.6 Cessation of business and transfer

In the event of **cessation of business**, the regime A data are deleted within ninety (90) days, subject to legal obligations; the regime B data follow article 12.4 of the Terms of Service, which then prevails over article B.3.

In the event of an **assignment, contribution or merger** entailing the transfer of the observation base, the assignee is bound, by the deed of assignment, by the same purposes, retention periods and limitations. Data subjects are informed of this by the update of the notice https://whoheld.com/trust/sellers-notice **before the processing is taken over**, and may object on that occasion.

Annex 1. Sub-processors

List as at October 1, 2026. Up-to-date version at https://whoheld.com/trust#subprocessors.

Sub-processor	Role	Regime	Location of processing
Supabase Pte. Ltd. (Amazon Web Services infrastructure)	Database, authentication, storage	A and B	**France, AWS region** `eu-west-3` **(Paris)**; company established in Singapore, teams distributed worldwide, standard contractual clauses (EU) 2021/914
Hostinger International Ltd.	Server running the collection	A and B	France (Paris), European Union; weekly backups of the instance in the Netherlands, European Union *(European Union, see note below)*
Resend	Service messages, alerts and evaluation onboarding series	A and B	Ireland, European Union (eu-west-1 region); company established in the United States, standard contractual clauses (EU) 2021/914
Anthropic Ireland, Limited (Ireland; processing in the United States by its parent company Anthropic, PBC)	Artificial intelligence assisted analysis (Ask WhoHeld: answers to Users' questions), on pseudonymised data and on the question typed by the User	A and B	**United States**; standard contractual clauses (EU) 2021/914
Vercel Inc.	Hosting of the web application	A and B	Germany (Frankfurt, fra1 region), global content delivery network; company established in the United States, standard contractual clauses (EU) 2021/914
Functional Software, Inc.	Reporting of technical errors of the web application, in order to diagnose and fix	B	**Germany (Frankfurt)**, Sentry's European Union data

Sub-processor	Role	Regime	Location of processing
(Sentry), San Francisco	failures: redacted error message and stack trace, technical identifier of the User account and of the Client, page concerned, browser, operating system, device type, language and time zone declared by the browser; never an email address, password or token, request content or seller identifier; no IP address retained and no geolocation, including inferred from the IP address; retention of ninety (90) days at most		region; company established in the United States, from where access is possible (support, account metadata): EU-US Data Privacy Framework and, failing that, standard contractual clauses (EU) 2021/914 (Sentry data processing addendum)
Google Cloud France SARL, 8 rue de Londres, 75009 Paris (Google Workspace)	The Publisher's business email: exchanges with the Client and its Users, invitations, support and evaluation onboarding	A and B	Google data centres, with no choice of region in the plan subscribed: transfers outside the European Union possible, governed by the Google Cloud data processing addendum (Cloud Data Processing Addendum: standard contractual clauses (EU) 2021/914; Google LLC certified under the EU-US Data Privacy Framework)

Hostinger offers instances outside the European Union (in particular United States, Singapore, Brazil) in addition to European instances: the commitment in article C.2 ("The data are hosted within the European Union") applies to this sub-processor only if the instance actually used is confirmed to be in the EU zone. This location is verified and recorded **before any go-live, including for a free evaluation**, and at each change of instance, in accordance with the procedure of article C.1; failing EU confirmation, this sub-processor is removed from regimes A and B until corrected. The instance in use is in Paris. Hostinger stores its weekly backups in the Netherlands, also in the European Union: this is not a transfer outside the Union.

No third-party audience measurement tool is deployed as at the date of this version; should one be installed, it would be added in accordance with the procedure of article C.1. The list is updated at each go-live, in accordance with that same procedure.

Annex 2. Security

Technical and organisational measures within the meaning of article 32 of the GDPR. **This annex forms part of the Contract.** The Publisher may modify it only in an equivalent or higher direction, under the conditions of article 7.2 of the Terms of Service.

Access control. Personal accesses, no shared account, least privilege. **Multi-factor authentication on administrative accesses and on the consoles of infrastructure sub-processors, implemented before any access is opened to the Client, including for a free evaluation**: any administrative privilege on the Platform requires a second factor verified during the session, checked by the database as well as by the application. Segregation of data between clients **at database level**

(isolation by row-level security policy) and not only at application level: an application error cannot expose another client's data. **The exception is the reference base of observed sellers**, common to all clients: it contains no Client Data and falls under regime A. Separation of technical roles; administration keys never exposed to the client application. Review of authorisations and revocation upon a team member's departure.

Encryption. TLS 1.2 minimum in transit; encryption at rest provided by the hosting infrastructure; secrets and keys outside the source code, no key in clear text in a repository.

Logging and monitoring. Logging of sensitive administrative operations: opening, extension, closure and conversion of accesses, invitations, removals and role changes of Users, switching of a Publisher administrator to a client's view. Logins are logged by the authentication provider, for the retention period of its offering. Continuous monitoring of production, with alerting on **absence of signal**: the system's silence triggers the alert, it is never read as normal operation. Logs kept for the published periods, aligned with the scheduled purges.

Backups. Automatic and daily; effective restoration depth = that of the tier subscribed with the host, provided on request; deletion at the end of a rotation cycle not exceeding ninety days. A **dated and documented restoration test is carried out no later than the effective date of the first Order Form**, then periodically.

Development and operations. Automated tests on each change, in continuous integration; a failure is dealt with before any go-live. An automated check verifies the database access rights after any change to the schema or to authorisations and fails if a client right is broken. Access to production restricted to authorised persons, from controlled workstations; **the separation of development and production environments is implemented no later than the effective date of the first Order Form**. Periodic and documented internal security review; external penetration test where the Order Form so provides.

Incidents. Procedure for qualification, containment, correction; notification to the client within forty-eight hours of becoming aware of a breach; **internal register of breaches** (article 33(5)), including those not notified; documented post-incident analysis.

Personnel. Confidentiality undertaking, awareness training, revocation of accesses at the end of an assignment.

An updated description, including work in progress, is set out in the Compliance Note provided on request under a confidentiality agreement.

End of the courtesy translation of the Personal Data Annex, version 8.3. The French version prevails.