Privacy Policy of the Crowd Hunter Service

(effective as of 8 May 2026)

This Privacy Policy explains how the Crowd Hunter Service (hereinafter referred to as the “Service” or “Crowd Hunter”) processes the personal data of Users and persons whose data are shared via the Service. This document fulfils the information obligations arising from Articles 13 and 14 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (GDPR). The Privacy Policy constitutes an integral supplement to the Terms and Conditions of the Service.

I. Controller of Personal Data

1. Administratorem danych osobowych jest Professionals Group spółka z ograniczoną odpowiedzialnością z siedzibą w Warszawie, ul. Grzybowska 80/82 lok. 700, 00-844 Warszawa, wpisana do rejestru przedsiębiorców KRS pod numerem 0000906685, NIP 5272922236, REGON 389986112 (dalej jako „Administrator" lub „my").

2. The Controller holds the status of an employment agency – KRAZ entry number: 23835.

3. Contact with the Controller on all matters concerning personal data:

a) email address: contact@crowdhunter.io

b) adres korespondencyjny: Professionals Group sp. z o.o., ul. Grzybowska 80/82 lok. 700, 00-844 Warszawa (z dopiskiem „Ochrona danych osobowych").

4. W przypadku danych Kandydatów przekazywanych potencjalnemu pracodawcy za pośrednictwem Serwisu, Professionals Group sp. z o.o. pozostaje administratorem danych w zakresie obsługi Serwisu oraz w zakresie nawiązania pierwszego kontaktu z Kandydatem. Z chwilą wyrażenia przez Kandydata zgody na udostępnienie jego danych Właścicielowi Projektu (kliknięcie „TAK" w dedykowanej wiadomości), firma publikująca ofertę pracy (Właściciel Projektu) staje się odrębnym administratorem danych Kandydata i samodzielnie decyduje o celach i sposobach ich dalszego przetwarzania w procesie rekrutacji. Każda ze stron przetwarza dane osobowe we własnym imieniu i na własną odpowiedzialność. Szczegółowo podział ten opisany jest w rozdziale V.

II. Data Protection Officer

1. The Controller has not appointed a Data Protection Officer within the meaning of Article 37 GDPR. The analysis of the nature, scope, and purposes of processing carried out did not reveal grounds requiring the appointment of a DPO.

2. For all matters relating to personal data (including the exercise of rights arising from the GDPR), please contact the Controller at the addresses indicated in Section I, item 3.

III. Categories of Personal Data Processed

We process the following categories of personal data – to the extent depending on the role in which you use the Service:

1. User identification, contact, and authentication data provided during Registration and use of the Account (including first name, last name, email address, phone number, position, password stored exclusively as an encrypted hash, avatar).

2. Company data (for Employer and Agency Accounts): identification data (name, NIP, KRAZ for Agencies), registered office address with geographical coordinates, presentation data (logo, description, specialisation, website), VAT status verification result.

3. Data relating to roles, status, and preferences in the Service: User type, role in the Team Account, Account status, verification flags with timestamps, preferred interface language.

4. Data of Candidates referred by Users: identification and contact data, CV (with professional information controlled exclusively by the Candidate), status in the recruitment process, anonymised IP address, and consent clause hash in the audit log.

5. Settlement data (when a Bonus payment is made): banking and identification data necessary for settlement (including account number, residential address, and possibly the PESEL/NIP of the Referring Party-consumer), financial transaction data, and Bonus Settlement Confirmations.

6. Technical and security data: client IP address and browser user-agent in security event audit logs, single-use cryptographic tokens for verification processes, data from anti-automation security mechanisms.

7. Data relating to consents and communication preferences: legal document acceptance markers (version, content hash, date, IP, user-agent), marketing consent status, transactional notification settings, cookie decisions (details in Section XI).

8. Data relating to use of the Service: usage counters (daily, weekly, hourly) used exclusively for enforcing the Quantitative Limits described in the Terms and Conditions (no IP, no fingerprint).

9. Data of persons visiting the Service without registration: anonymousId generated server-side, cookie decisions, salted hash of the IP address, user-agent, visit timestamp.

Special category data (so-called sensitive data). As a rule, we do not collect or require Users to provide special categories of personal data referred to in Article 9 GDPR (e.g., health data, political views, religious beliefs, racial origin, trade union membership, etc.). Please do not include such information in your profile or in documents (CVs) submitted via the Service, unless it is necessary and you provide a separate, explicit consent for this purpose. Should we receive sensitive data without explicit consent, the Controller reserves the right to delete it immediately.

IV. Data of Referred Persons (Obligation under Article 14 GDPR)

If your personal data have been transmitted to the Service by another User as part of a candidate referral, we hereby fulfil our information obligation towards you under Article 14 GDPR. We inform you that:

1. Source of data. We received the data from a registered User (the Referring Party), who in the referral form declared that they had agreed with you the transfer of this data to the Service.

2. Data controller. The controller of your data for the purposes of handling the referral process (before you give your consent to participate) is Professionals Group sp. z o.o.

3. Scope of data. The data typically include first name, last name, contact details (email, phone), and professional information provided for recruitment purposes (including a CV file).

4. Identity of the Referring Party. As part of fulfilling the information obligation regarding the source of data (Article 14(2)(f) GDPR), we will inform you of the first name, last name, email address, and company name of the Referring Party.

5. Purposes and legal basis. We will process the data:

a) Stage 1 (first contact, request for consent) – on the basis of Article 6(1)(f) GDPR (the legitimate interest of the Controller consisting in sourcing candidates for clients);

b) Stage 2 (disclosure of data to the Project Owner) – on the basis of Article 6(1)(a) GDPR (the Candidate's voluntary consent expressed by clicking 'YES' in the message).

6. **Right to refuse.** You may refuse to participate in the process at any time by selecting the 'NO' option in the dedicated message, or – if consent has already been given – by using the one-click consent withdrawal link. Details in Section V.
7. **Time of providing information.** In accordance with Article 14(3) GDPR, we fulfil the information obligation upon first contact, i.e., in the message sent immediately after your data are entered into the Service by the Referring Party.
8. **Your rights.** You have all the rights described in Section X, including the special right to object to the processing of data obtained from a third party (Article 21 GDPR).

V. Purposes and Legal Bases for Data Processing

Your personal data are processed for the following purposes and on the following legal bases:

1. Maintaining the User Account and providing the Services of the Service (registration, authentication, login, profile editing, communication within the Service, settlements, operational notifications).

Legal basis: *Article 6(1)(b) GDPR – performance of the Agreement for the Provision of Services by Electronic Means concluded by acceptance of the Terms and Conditions.*

2. Account security and identity verification (verification of email address and phone number, handling email and password changes, password reset, detection of Account takeover attempts, sending security alerts).

Legal basis: *Article 6(1)(b) GDPR (performance of the Agreement) and Article 6(1)(f) GDPR (legitimate interest – prevention of unauthorised access).*

3. Verification of the company's tax status (KYC). Automatic or triggered query to the public register of the White List of VAT taxpayers of the Polish Ministry of Finance in order to confirm the identity and tax status of the Employer or Agency.

Legal basis: *Article 6(1)(f) GDPR (legitimate interest – KYC/AML, counterparty verification) and – indirectly – Article 6(1)(c) GDPR (due diligence in B2B transactions, Act of 12 April 2019 on split payment).*

4. Candidate Referral Programme (crowdstaffing) – implementation of the process of referring Candidates to Projects, contacting the Candidate, obtaining their consent, disclosing data to the Project Owner.

Legal basis:

a) Stage 1 (first contact with the Candidate) – Article 6(1)(f) GDPR (legitimate interest – sourcing candidates for clients). We have carried out a balancing test demonstrating that our interest does not infringe the rights and freedoms of the Candidate, as the condition for all further actions is the Candidate's consent;

b) Stage 2 (disclosure of data to the Project Owner) – Article 6(1)(a) GDPR (the Candidate's voluntary consent).

5. Information obligation towards the Candidate – source of data (Article 14 GDPR). Disclosure to the Candidate of information about the identity of the Referring Party (first name, last name, email address, company name).

Legal basis: *Article 6(1)(b) GDPR (performance of the Agreement – element of the referral service) and Article 6(1)(c) GDPR (legal obligation arising from Article 14(2)(f) GDPR). In view of Recital 43 GDPR (lack of voluntariness), the legal basis is not consent.*

6. Publication of Projects. Making Project content available to other Users of the Service and – in certain cases – to public visitors.

Legal basis: *Article 6(1)(b) GDPR (performance of the Agreement).*

7. Internal communication between companies. Handling the exchange of messages between Users within the Service and email notifications about new messages.

Legal basis: *Article 6(1)(b) GDPR (performance of the Agreement) and Article 6(1)(f) GDPR (handling recruitment processes).*

8. Handling employment and Bonus settlements. Tracking the planned employment date, reminders about employment confirmation and the approaching end of the Guarantee Period, bilateral Bonus Settlement Confirmation, settlement of the Bonus and Commission.

Legal basis: *Article 6(1)(b) GDPR (performance of the Agreement) and Article 6(1)(c) GDPR (Act of 29 September 1994 on Accounting, Tax Ordinance – retention of accounting documents for 5 years).*

9. Company Team Invitations. Sending an email invitation to persons invited by the Team Account Admin and handling the activation process of the invited Account.

Legal basis: *Article 6(1)(b) GDPR (the invitation constitutes an offer to conclude a contract within the meaning of the Civil Code).*

10. Agency Public Profile. Making the Recruitment Agency's data available on the public page https://www.crowdhunter.io/ on the basis of the explicit, voluntary consent expressed in the Account settings.

Legal basis: *Article 6(1)(a) GDPR (consent).*

11. Marketing communication. Sending marketing messages (alerts about new job offers, information about new Service features) exclusively to Users who have given explicit consent in the registration form or in the Account settings.

Legal basis: *Article 6(1)(a) GDPR (consent) and Article 398 of the Act of 12 July 2024 – Electronic Communications Law (consent to use terminal equipment and automated calling systems for direct marketing purposes).*

12. Register of consents to legal documents. Maintaining an accountable record of acceptance of the Terms and Conditions and Privacy Policy (Article 7 GDPR) and sending pre-notices 14 days before the entry into force of new versions of documents (Articles 12/13 GDPR).

Legal basis: *Article 6(1)(c) GDPR (legal obligation arising from Articles 5(2), 7(1), and 12–14 GDPR).*

13. Account closure and exercise of the right to erasure (Article 17 GDPR). Handling Account closure requests (self-service or initiated by the Service Admin), anonymisation of identifying data, settlement of open Bonuses (transfer or forfeiture), Account closure survey.

Legal basis: *Article 17(1) GDPR (right to erasure), Article 6(1)(b) GDPR (performance of the Agreement) and Article 6(1)(c) GDPR (retention of the audit log and accounting data despite Account closure).*

14. Cookie consent handling. Collecting, recording, and honouring user preferences regarding optional cookies.

Legal basis: *Article 6(1)(c) GDPR (Articles 5(2) and 7 GDPR – accountability) and Article 394 of the Act of 12 July 2024 – Electronic Communications Law (storage of information on the User's terminal equipment).*

15. Quantitative restrictions (rate limiting) and abuse prevention. Recording usage counters (by User UID) for the purpose of enforcing the Quantitative Limits described in the Terms and Conditions.

Legal basis: *Article 6(1)(f) GDPR (protection of the platform against abuse).*

16. Handling enquiries and complaints. Responding to enquiries sent to contact@crowdhunter.io and processing complaints in accordance with the procedure described in the Terms and Conditions.

Legal basis: *Article 6(1)(b) GDPR (performance of the Agreement) and Article 6(1)(f) GDPR (user support).*

Obligation to provide data. Providing data is voluntary, however in certain cases it is necessary to conclude or perform the Agreement or to use a specific Service functionality (e.g., without an email address and phone number we will not create an Account). Failure to provide data may result in the inability to achieve a given purpose (in accordance with Article 13(2)(e) GDPR).

Automated decisions and profiling. We do not apply automated decision-making within the meaning of Article 22 GDPR, including profiling that would produce legal effects concerning you or similarly significantly affect you. Every recruitment process involves an assessment carried out by recruiters or representatives of the Employer. Automated classifications applied in the Service (e.g., the Account trust level determining Quantitative Limits) are purely operational in nature and do not produce legal effects.

VI. Recipients of Personal Data

Your personal data are not sold or used in an unauthorised manner. They may be disclosed exclusively to the following categories of recipients, with respect to the principle of data minimisation (Article 5(1)(c) GDPR):

1. Processors acting on behalf of the Controller (on the basis of data processing agreements compliant with Article 28 GDPR):

a) Google LLC – provider of the Firebase platform (Firebase Authentication, Cloud Firestore, Cloud Storage) used for hosting the Service and storing Users' and Candidates' data;

b) Google LLC (Google Maps Platform) – geocoding of addresses entered by Users (company registered office addresses, residential addresses of natural persons) in order to display coordinates for the Service's functionality;

c) Google LLC (Google reCAPTCHA Enterprise) – protection of the phone number verification process against bots;

d) Google LLC (Firebase Phone Auth) – delivery of SMS messages with one-time verification codes to the User's phone number;

e) Twilio Inc. / Twilio SendGrid Inc. – delivery of transactional and marketing email messages (registration confirmations, messages to Candidates, security alerts, notifications about new messages, marketing messages, and others);

f) Vercel Inc. – provider of application infrastructure (application hosting, server-side runtime);

g) other IT entities providing infrastructure maintenance, technical support, monitoring – to the extent necessary for the performance of the entrusted tasks, each time on the basis of a data processing agreement guaranteeing a level of protection consistent with the GDPR.

2. Recipients acting as separate data controllers:

a) Project Owner (Employer/Agency) – upon the Candidate's consent to the disclosure of data in the referral process (the 'YES' option in the dedicated message), the Candidate's data are disclosed to the Project Owner, who from that moment becomes a separate data controller within their own recruitment process. The Project Owner then bears the obligation to comply with all GDPR requirements, including the information obligation under Article 13 GDPR;

b) Candidate receiving the message – as part of fulfilling the information obligation under Article 14(2)(f) GDPR, the Candidate is provided with the data of the Referring Party (first name, last name, email, company name). The Candidate becomes an independent controller of this data to the extent necessary to remember the source of the referral;

c) Ministry of Finance of the Republic of Poland – when verifying the company's tax status (VAT White List), a query containing the company's NIP number is transmitted; the Ministry, as the operator of the public register, is a separate controller of the data contained in that register.

3. Public recipients: in the event of activation of the Public Profile by the Recruitment Agency, the data disclosed in the Profile (company name, NIP, KRAZ, logo, address, description, specialisation) are visible to all visitors of the Service and may be indexed by search engines.

4. Public authorities entitled to obtain data on the basis of legal provisions – to courts, prosecutors' offices, the Police, the President of the PDPA, tax administration, and other authorities exclusively within the scope and on the conditions specified by legal provisions. Every such request is subject to legal verification before data are disclosed.

5. Law firms and statutory auditors, tax advisors, audit firms – within the scope of providing advisory services to the Controller, to the extent necessary for the performance of their duties and under a confidentiality clause.

We do not sell data to any marketing entities, data brokers, or aggregators. The list of processors may be subject to updates; information about the current list is available upon request sent to contact@crowdhunter.io.

VII. Transfers of Data Outside the European Economic Area (EEA)

1. In the context of using the services of certain processors, your personal data may be transferred to third countries outside the EEA, in particular to the United States. This applies in particular to:

a) Google LLC (Firebase, Google Maps, reCAPTCHA, Firebase Phone Auth) – the provider is headquartered in the USA; data may be stored in data centres in the USA and processed globally in accordance with the Google Cloud infrastructure;

b) Twilio Inc. / Twilio SendGrid Inc. – the provider is headquartered in the USA;

c) Vercel Inc. – the provider is headquartered in the USA;

d) Ministry of Finance of the Republic of Poland – located in the EEA (Poland) – no transfer outside the EEA;

e) Independently of the main transfer directions indicated above, the infrastructure of global providers (in particular Google Cloud) may, under certain conditions, replicate data to other geographical regions outside the EEA (e.g., Asia, South America) exclusively for purposes arising from the high-availability and data recovery architecture (DR/HA). Every such transfer takes place under the same safeguards as the transfers to the USA described in item 2.

2. In order to ensure an adequate level of data protection for transfers to the USA, the following safeguards have been applied:

a) Standard Contractual Clauses (SCCs) approved by the European Commission pursuant to Article 46 GDPR, incorporated into the data processing agreements concluded with providers;

b) participation of providers in the EU-US Data Privacy Framework (DPF, the successor to Privacy Shield) – as of the date of entry into force of this Policy, Google LLC and Twilio Inc. are active participants in the DPF (public register: dataprivacyframework.gov). We periodically verify Vercel Inc.'s participation status; in the absence of DPF certification, transfers take place exclusively on the basis of the SCCs described in point a;

c) additional technical and organisational measures (TOMs) recommended by the European Data Protection Board:

- encryption of transmissions and stored data;
- pseudonymisation of audit data (IP anonymisation, hashing of sensitive values);
- minimisation of the scope of transmitted data;
- verification of providers' privacy policies and security practices.

3. You have the right to obtain a copy of the implemented clauses and other transfer safeguards by contacting the Controller at contact@crowdhunter.io.

VIII. Data Retention Period

We process personal data for the period necessary to achieve the purposes indicated in Section V, and thereafter – to the extent justified by legal obligations or our legitimate interests – for the periods indicated below. The detailed retention policy elaborating on these principles is maintained in the internal Register of Processing Activities (RPA) and made available to supervisory authorities upon request.

1. **User Account data and history of changes.** For the entire duration of the Agreement. After Account closure, identifying data are anonymised immediately; anonymised records together with the audit log and history of Account data changes are retained for up to 6 years (limitation period for claims and accounting obligations). Unactivated Accounts are physically deleted without anonymisation at the time of closure. The Account closure survey together with the closure audit log is retained for 6 years from the date of closure.
2. **Data of referred Candidates.** We apply differentiated retention rules depending on the status of the referral – from 7 days (refusal or withdrawal of consent) and 14 days (no response), through 9 months (Referral Validity Period), up to 6 years from the end of the year of employment for data necessary for Bonus settlement and accounting obligations. The consent audit log is retained for 6 years from the date of deletion of the Candidate's data; at the time of deletion of the Candidate's data, the email field is anonymised, while the remaining fields (date, clause version, anonymised IP) are retained for accountability purposes (Article 5(2) GDPR).
3. **Register of consents to legal documents (Terms and Conditions, Privacy Policy).** 6 years after termination of the Agreement – as proof of acceptance of the document content in a specific version (Article 7(1) GDPR).
4. **Single-use tokens and invitations.** Email change, password reset, and privilege promotion tokens – from 60 minutes to 24 hours (single-use). Team Invitations – until first login or deletion by the Admin; periodic review after 90 days without activation.
5. **Cookies and cookie consent register.** Session and preference cookies – from the browser session duration up to 5 days. Cookie recording the cookie consent decision client-side – 365 days. Entries in the cookieConsentLog collection – 6 years from recording (Article 7 GDPR). Details in Section XI.

6. **Technical and security data.** Rate limit counters – up to 30 days (daily bucket), 8 weeks (weekly), 7 days (hourly). NIP verification cache in the White List register – 30 days. System logs and technical security data – up to 12 months, longer only when they constitute evidence in ongoing proceedings.
7. **Accounting and tax documentation (invoices, receipts, settlement agreements, Bonus Settlement Confirmations).** 5 full tax years counted from the end of the year in which the accounting event occurred – in accordance with Article 74(2) of the Act of 29 September 1994 on Accounting and Article 86 § 1 of the Tax Ordinance.

Upon expiry of the indicated periods, personal data are permanently deleted or anonymised in an irreversible manner.

IX. Security Measures

1. The Controller applies technical and organisational measures ensuring the protection of personal data appropriate to the risk identified for each category of processing, in accordance with Article 32 GDPR. Among the measures applied are in particular:
   a) **Technical measures:** encryption of transmissions and data stored in the infrastructure, password hashing, authenticated cookie sessions with HttpOnly, Secure and SameSite attributes, single-use cryptographic tokens for security operations, anonymisation of IP addresses in audit logs, hashing of consent clauses as proof of integrity, bot protection in verification processes, rate limiting of sensitive operations, server-side input data validation.
   b) **Organisational measures:** role-based access control (Admin / Editor / Viewer) with server-side enforcement of permissions, centralised Dashboard access gateways, audit log of personal data changes and permission changes, two-step User verification (email + SMS), two-step verification of email address changes, personal data breach response procedures in accordance with Articles 33 and 34 GDPR, versioning of legal documents with re-acceptance requirement upon significant content changes, periodic reviews of Account trust levels and Quantitative Limits.

A detailed list of technical measures applied (including protocol versions, token lengths, and algorithm parameters) is maintained in the Register of Processing Activities (Section XII) and made available to supervisory authorities upon request.

2. **Notification of a breach (Article 34 GDPR).** In the event of a personal data breach likely to result in a high risk to your rights or freedoms, we will notify you without undue delay, to the email address associated with the Account or to another available contact channel. The notification will include: a description of the nature of the breach, the contact details of the Controller (and, if necessary, details of other contact points), a description of the likely consequences of the breach, and a description of the measures taken or proposed by the Controller to address the breach, including to minimise its potential adverse effects. Independently of notifying the data subjects, the Controller reports breaches to the President of the PDPA within 72 hours of becoming aware of them (Article 33 GDPR), where the statutory conditions are met.

X. Rights of Data Subjects

In connection with our processing of your personal data, you have the following rights:

1. **Right of access (Article 15 GDPR) –** the right to obtain confirmation of whether we process your data, and if so – the right to access them, obtain a copy thereof, and receive information about the purposes, categories, recipients, and retention periods.

2. **Right to rectification (Article 16 GDPR) –** the right to request rectification of inaccurate data or completion of incomplete data. Most Account data can be edited independently in the settings.
3. **Right to erasure ("right to be forgotten") (Article 17 GDPR) –** the right to request erasure of data in certain situations (when data are no longer needed, when consent is withdrawn, when processing is unlawful, etc.). This right is not absolute – we may refuse erasure to the extent that data are necessary for the performance of a legal obligation (e.g., accounting documentation) or for the establishment, exercise, or defence of claims. In such a case, we will provide reasoning for the refusal. In the Service, Account closure results in immediate anonymisation of identifying data – see Section VIII, item 1.
4. **Right to restriction of processing (Article 18 GDPR) –** the right to request a temporary suspension of processing in certain cases (e.g., when you contest the accuracy of the data pending their verification).
5. **Right to data portability (Article 20 GDPR) –** the right to receive, in a structured, commonly used format (e.g., CSV), data that you have provided to us, or to request that they be transmitted directly to another controller (if technically feasible). The right applies to data processed on the basis of consent or a contract.
6. **Right to object (Article 21 GDPR) –** the right to object to processing based on the legitimate interest of the Controller (Article 6(1)(f) GDPR) on grounds relating to your particular situation. In the case of direct marketing, the objection requires no justification and is always respected.

Special right of objection for Candidates (Article 21(1) GDPR): if your data have been transmitted to the Service by the Referring Party, you may at any time object to further processing – we will cease processing unless we demonstrate the existence of overriding legitimate grounds (e.g., defence against claims).

7. **Right to withdraw consent (Article 7(3) GDPR) –** if processing is based on consent, you may withdraw it at any time. Withdrawal of consent does not affect the lawfulness of processing carried out prior to its withdrawal. In the Service:
   - **a)** marketing consents – deactivation of the relevant toggles in the Account settings;
   - **b)** Candidate's consent to the disclosure of data to the Project Owner – one-click link in the consent confirmation message or contact with the Controller;
   - **c)** Agency's consent to the Public Profile – deactivation of the 'Public profile' toggle in the Account settings;
   - **d)** cookie consents – the cookie settings panel in the footer of the Service.
8. **Right not to be subject to a decision based solely on automated processing (Article 22 GDPR) –** in accordance with Section V, the Controller does not apply such decisions.
9. **Right to lodge a complaint with a supervisory authority.** If you consider that we are processing data in violation of the regulations, you have the right to lodge a complaint with a supervisory authority, which in Poland is the President of the Personal Data Protection Office (PDPA), ul. Stawki 2, 00-193 Warsaw, www.uodo.gov.pl. You may also direct a complaint to the supervisory authority in another EU Member State (at your place of habitual residence, workplace, or place of the alleged infringement). We encourage you, however, to contact the Controller first – we will endeavour to resolve the matter amicably.

How to exercise your rights. All requests may be directed to contact@crowdhunter.io or in writing to the Controller's registered office address. We respond without undue delay, no later than within one month of receiving the request; if necessary, this period may be extended by a further two months, of which we will inform you along with the reasoning. The exercise of rights is free of charge, except for requests that are

manifestly unfounded or excessive (Article 12(5) GDPR). Before fulfilling a request, we may ask for additional information for the purpose of identity verification.

XI. Cookies and Similar Technologies

1. **Current status.** The Crowd Hunter Service does not currently use optional cookies – neither analytical, marketing, nor profiling ones. We do not use any external tracking tools either. The only cookies used by the Service are cookies necessary for its proper operation.
2. Necessary cookies used in the Service:
   - **a)** `__session` – Firebase Authentication session cookie. Purpose: maintaining the User's logged-in state. Lifetime: 5 days. Flags: HttpOnly, Secure, SameSite=Lax;
   - **b)** `ch_cookie_consent` – cookie recording the User's cookie decision. Purpose: remembering the choice and hiding the cookie banner on subsequent visits. Lifetime: 365 days. Flags: SameSite=Lax, Secure (in production environment), httpOnly=false (necessary to read the decision client-side without an additional round-trip);
   - **c)** `NEXT_LOCALE` – interface language selection cookie. Purpose: preserving the language preference between visits. Lifetime: browser session.

The legal basis for the use of necessary cookies is Article 6(1)(f) GDPR (legitimate interest – provision of the service requested by the User) and Article 394(3)(2) of the Act of 12 July 2024 – Electronic Communications Law (exemption from the consent obligation for cookies necessary for the provision of the service).

3. **Cookie decision register.** Every User decision (acceptance, rejection, update, withdrawal) is recorded in the cookieConsentLog collection maintained by the Controller – in accordance with the accountability obligation (Article 7 GDPR). The register contains: anonymousId (UUIDv4 generated server-side, not correlated with the IP address), User UID (if logged in), flag for acceptance of optional cookies, action type, source (banner/settings/footer), consent version, salted SHA-256 hash of the IP address, user-agent, timestamp.
4. **Cookie consent management.** Should optional cookies be introduced in the future, the User will be asked to give consent in a separate banner, and their decision will be recorded in the register. The consent management mechanism is fully implemented by the Controller internally – we do not use external Consent Management Platforms (CMPs). The User may withdraw consent or change their preferences at any time using the 'Cookie settings' link available in the footer of the Service.
5. **Browser settings.** Independently of the consent mechanism implemented by the Controller, you may manage cookies at the level of your web browser. Most browsers allow cookies to be blocked, filtered, or automatically deleted. Detailed information can be found in the 'Help' section of the relevant browser. Blocking necessary cookies may cause the Service to malfunction (e.g., inability to log in).
6. **Server logs.** Independently of cookies, the servers operating the Service automatically log HTTP requests, including the device's IP address, timestamp, browser identifier (user-agent), and response code. We use this data exclusively for technical and security purposes (error diagnosis, attack detection) on the basis of Article 6(1)(f) GDPR. Logs are retained for a maximum of 12 months.

XII. Register of Processing Activities (RPA)

1. The Controller maintains a Register of Processing Activities in accordance with Article 30 GDPR, describing in detail each data processing activity, its purpose, legal basis, categories of data subjects, categories of

data, categories of recipients, planned retention periods, and the technical and organisational measures applied.

2. The RPA is made available to:

a) the President of the Personal Data Protection Office and other competent supervisory authorities upon their request;

b) data subjects – to the extent necessary for the exercise of their rights arising from the GDPR – upon request sent to contact@crowdhunter.io.

XIII. Updates to the Privacy Policy

1. This Privacy Policy may be subject to updates in order to reflect changes in the way data are processed, changes in legal provisions, or in response to recommendations of supervisory authorities.

2. We will notify Users of significant changes to the Policy at least 14 days in advance of the date of entry into force of the new version – by means of an email message to the address associated with the Account and by a clear notice on the Service's website. If the User does not accept the changes, they have the right to close the Account before the date of entry into force of the changes.

3. The current version of the Privacy Policy is always available at https://www.crowdhunter.io/. The date of the last update and the date of entry into force are indicated at the beginning of the document.

4. This Privacy Policy has been drawn up in the Polish and English languages. In the event of discrepancies between the language versions, the Polish-language version shall prevail.