🔐 PRIVACY POLICY – Refcruiter

Last updated: February 6, 2026

Effective Date: February 6, 2026

This Privacy Policy describes how Refcruiter ("we", "us", "our") collects, uses, processes, and protects your personal information when you use our job board platform (the "Service").

This policy complies with:

- EU General Data Protection Regulation (GDPR)
- California Consumer Privacy Act (CCPA) / California Privacy Rights Act (CPRA)
- Brazil's Lei Geral de Proteção de Dados (LGPD)
- Canada's Personal Information Protection and Electronic Documents Act (PIPEDA)
- UK Data Protection Act 2018 / UK GDPR
- Australia's Privacy Act 1988
- Other applicable international privacy laws

---

1. DATA CONTROLLER & CONTACT INFORMATION

Data Controller:

Mykyta Usatenko and Eduard Shuliak

Operating as: Refcruiter

Location: Poland

Website: https://refcruiter.willfind.org

Contact for Privacy Matters:

- Emails:

Mykyta Usatenko: mykyta.usatenko@willfind.org

Eduard Shuliak: eduard.shuliak@willfind.org

• Founders: mykyta.usatenko@willfind.org, eduard.shuliak@willfind.org

• Response Time: Within 30 days (GDPR) / 45 days (CCPA)

EU Representative: Available upon request for EU data subjects

UK Representative: Available upon request for UK data subjects

---

2. SCOPE & DEFINITIONS

This policy applies to:

• Job Seekers/Candidates: Individuals who browse jobs, create accounts, or submit applications

• Employers/Recruiters: Individuals/companies who post jobs and review applications

• Website Visitors: Anyone who accesses our Service

• Guest Users: Individuals who apply to jobs without creating an account

Personal Data: Any information relating to an identified or identifiable individual.

---

3. PERSONAL DATA WE COLLECT

3.1 Data You Provide Directly

When you use our Service, you may provide:

For All Users:

• Account Information: Name, email address, password (hashed), username

• Profile Information: First name, last name, professional title, location

• Contact Details: Email address, phone number (optional)

• Communication Data: Messages sent to support, feedback, inquiries

For Job Seekers/Candidates:

• Resume/CV: Uploaded files containing work history, education, skills, contact info

• Application Data: Cover letters, responses to application questions

• Job Preferences: Desired job types, locations, salary expectations

• Professional Information: LinkedIn profile, GitHub, portfolio URLs

For Employers/Recruiters:

• Company Information: Company name, website, logo, description, size

• Job Posting Data: Job titles, descriptions, requirements, salary ranges, locations

• Billing Information: Company address, VAT/Tax ID (processed via Stripe)

• Payment Data: Credit card information (handled entirely by Stripe, not stored by us)

3.2 Data Collected Automatically

• Technical Data: IP address, browser type, device type, operating system

• Usage Data: Pages visited, time spent, click patterns, referring URLs

• Cookies & Tracking: See our Cookie Policy for details

• Log Data: Access times, error logs, security events

3.3 Data from Third Parties

• OAuth Providers: If you use social login (Google, LinkedIn, GitHub), we receive

basic profile info (name, email, profile photo) per your OAuth consent

• Payment Processors: Stripe provides transaction confirmations and payment metadata

• Email Verification: We may use email validation services to verify email addresses

---

4. HOW WE USE YOUR PERSONAL DATA

4.1 Service Provision & Contract Performance

• Account Management: Creating, maintaining, and securing your account

• Job Applications: Processing and delivering your applications to employers

• Job Posting: Publishing and managing job listings

• Communication: Sending transactional emails (application confirmations, job matches)

• Payment Processing: Processing subscriptions and job posting fees via Stripe

4.2 Legal Obligations & Compliance

• Tax & Accounting: Maintaining records for tax compliance

• Fraud Prevention: Detecting and preventing fraudulent activities

• Legal Requests: Responding to lawful requests from authorities

• Terms Enforcement: Investigating violations of our Terms of Service

4.3 Legitimate Interests

• Service Improvement: Analyzing usage to enhance features and user experience

• Security: Monitoring for security threats and preventing unauthorized access

• Customer Support: Responding to inquiries and resolving issues

• Business Operations: Internal reporting, analytics, and optimization

4.4 With Your Consent

• Marketing Communications: Sending newsletters and promotional emails (opt-in only)

• Non-Essential Cookies: Analytics and marketing cookies (opt-in via cookie banner)

• Social Media Integration: Connecting your social profiles (optional)

---

5. LEGAL BASIS FOR PROCESSING (GDPR Article 6)

We process your data based on:

• Contract Performance (Art. 6(1)(b)): Necessary to provide our Service and fulfill

our agreement with you (e.g., delivering job applications, processing payments)

• Consent (Art. 6(1)(a)): Where you explicitly agree (e.g., marketing emails,

optional cookies, social login)

• Legitimate Interest (Art. 6(1)(f)): For improving our Service, ensuring security,

fraud prevention, and business operations (balanced against your rights)

• Legal Obligation (Art. 6(1)(c)): When required by law (e.g., tax records,

responding to court orders)

You have the right to object to processing based on legitimate interest.

---

6. JOB APPLICATIONS & DATA SHARING WITH EMPLOYERS

6.1 How Applications Work

When you apply for a job:

1. Your resume/CV and application data are uploaded to our secure Supabase storage

2. The employer/recruiter gains access to view and download your application materials

3. Your name, email, resume, and cover letter are shared with the employer

4. The employer becomes an independent data controller for your application data

6.2 Employer Responsibilities (Data Processing Agreement)

Employers who receive your applications act as independent Data Controllers and must:

• Comply with applicable privacy laws (GDPR, CCPA, etc.)

• Process your data only for recruitment purposes

• Maintain appropriate security measures

• Respect your data subject rights

• Delete your data when no longer needed for recruitment

6.3 Our Role as Data Processor

For application data, Refcruiter acts as a Data Processor on behalf of employers:

• We provide the technical infrastructure to store and deliver applications

• We process data only per employer instructions (delivering applications)

• We maintain security measures (encryption, access controls)

• We facilitate data subject rights requests related to applications

6.4 Guest Applications (Non-Registered Users)

You can apply to jobs without creating an account by providing:

• First name, last name, email address

• Resume/CV file

• Optional cover letter

Guest applications are treated identically to registered user applications. Your data is shared with the employer and stored for 90 days (see Section 8).

---

7. WHO WE SHARE YOUR DATA WITH

7.1 Employers/Recruiters (When You Apply)

Your application data is shared with employers per Section 6.

7.2 Service Providers & Sub-Processors

We engage trusted third parties to support our Service:

• Supabase (US): Cloud storage for resumes/CVs and database hosting

→ Privacy Policy: https://supabase.com/privacy

→ Safeguards: Standard Contractual Clauses (SCCs), encryption at rest and in transit

• Stripe (US): Payment processing for job posting subscriptions

→ Privacy Policy: https://stripe.com/privacy

→ Safeguards: PCI-DSS Level 1 compliant, EU-US Data Privacy Framework

• Typesense (Self-Hosted): Job search indexing (data stored on our infrastructure)

→ Privacy Policy: https://typesense.org/privacy

→ Safeguards: Self-hosted, data remains under our control

• Email Service Provider: Transactional emails (account verification, notifications)

→ We use secure SMTP providers compliant with data protection laws

7.3 Legal & Regulatory Authorities

We may disclose data when required by law:

• Court orders, subpoenas, or legal processes

• Requests from law enforcement or regulatory agencies

• To protect our rights, property, or safety

• To enforce our Terms of Service

7.4 Business Transfers

In the event of a merger, acquisition, or sale of assets:

• Your data may be transferred to the acquiring entity

• You will be notified via email and prominent website notice

• The new entity will be bound by this Privacy Policy

7.5 We Do NOT Sell Your Data

We do not sell, rent, or trade your personal information to third parties for monetary consideration. (CCPA: We have not sold personal information in the past 12 months.)

---

8. DATA RETENTION & DELETION

8.1 Active Accounts

• Account Data: Stored while your account is active and for 90 days after account deletion

• Profile Information: Retained until you delete your account

• Application History: Stored for 90 days after application submission

• Communication Logs: Stored for 2 years for customer support and legal compliance

8.2 Resumes/CVs & Application Files

• Retention Period: 90 days from application submission date

• Automatic Deletion: Our system automatically deletes application files after 90 days

• Employer Access: Employers should download applications within 90 days

• Early Deletion: You can request immediate deletion (see Section 10)

8.3 Job Postings

• Active Jobs: Stored while the job is active and for 90 days after expiration

• Expired Jobs: Archived for 1 year, then anonymized for analytics

8.4 Payment & Billing Records

• Transaction Records: Stored for 7 years per tax and accounting regulations

• Invoices: Retained for 7 years (legal requirement)

• Payment Card Data: Never stored by us (handled entirely by Stripe)

8.5 Logs & Security Data

• Access Logs: Retained for 90 days

• Security Incident Logs: Retained for 2 years

• Audit Trails: Retained for 7 years per legal requirements

8.6 Account Deletion

When you delete your account:

1. Your profile is immediately deactivated

2. Personal data is deleted within 90 days

3. Anonymized analytics data may be retained indefinitely

4. Legal/financial records retained per retention schedules above

---

9. INTERNATIONAL DATA TRANSFERS

9.1 Data Location

Your data may be processed and stored in:

• European Union: Our primary database servers (via Supabase EU region)

• United States: Backup servers, Stripe payment processing, third-party services

• Other countries: Where our service providers operate

9.2 Transfer Safeguards (GDPR Chapter V)

For transfers outside the EU/EEA, we ensure adequate protection via:

• Standard Contractual Clauses (SCCs): EU Commission-approved contracts with processors

• EU-US Data Privacy Framework: For US-based processors certified under the framework

• Adequacy Decisions: Transfers to countries with EU adequacy decisions

• Your Explicit Consent: Where applicable

9.3 Your Rights Regarding International Transfers

You have the right to:

• Request information about transfer safeguards

• Object to transfers to specific countries

• Request a copy of SCCs or other safeguards

• Contact

Mykyta Usatenko: mykyta.usatenko@willfind.org

Eduard Shuliak: eduard.shuliak@willfind.org

for details

---

10. YOUR PRIVACY RIGHTS

10.1 Rights Under GDPR (EU/UK/EEA Residents)

You have the right to:

• Access (Art. 15): Obtain a copy of your personal data we hold

• Rectification (Art. 16): Correct inaccurate or incomplete data

• Erasure / "Right to be Forgotten" (Art. 17): Request deletion of your data

• Restriction (Art. 18): Limit how we process your data

• Data Portability (Art. 20): Receive your data in a machine-readable format

• Object (Art. 21): Object to processing based on legitimate interests

• Withdraw Consent (Art. 7(3)): Withdraw consent for consent-based processing

• Lodge a Complaint (Art. 77): File a complaint with your supervisory authority

10.2 Rights Under CCPA/CPRA (California Residents)

You have the right to:

• Know: Request disclosure of personal information collected, used, and shared

• Access: Obtain a copy of your personal information

• Delete: Request deletion of your personal information

• Correct: Request correction of inaccurate information (CPRA)

• Opt-Out of Sale/Sharing: We don't sell data, but you can opt out if practices change

• Opt-Out of Automated Decision-Making: We don't use automated decision-making

• Non-Discrimination: We won't discriminate against you for exercising your rights

Designated Methods to Submit Requests:

• Email:

Mykyta Usatenko: mykyta.usatenko@willfind.org

Eduard Shuliak: eduard.shuliak@willfind.org

with subject "CCPA Request"

• Response Time: 45 days (may extend to 90 days with notice)

10.3 Rights Under LGPD (Brazil Residents)

You have the right to:

• Confirmation and access to your data

• Correction of incomplete or inaccurate data

• Anonymization, blocking, or deletion

• Data portability

• Information about public/private entities with whom data is shared

• Information about the possibility of denying consent

• Revocation of consent

Contact:

Mykyta Usatenko: mykyta.usatenko@willfind.org

Eduard Shuliak: eduard.shuliak@willfind.org

with subject "LGPD Request"

10.4 Rights Under PIPEDA (Canada Residents)

You have the right to:

• Access your personal information

• Challenge the accuracy and completeness of your information

• Withdraw consent (where consent is the basis for processing)

• File a complaint with the Privacy Commissioner of Canada

Contact:

Mykyta Usatenko: mykyta.usatenko@willfind.org

Eduard Shuliak: eduard.shuliak@willfind.org

with subject "PIPEDA Request"

10.5 How to Exercise Your Rights

To exercise any of these rights:

1. Send an email to:

Mykyta Usatenko: mykyta.usatenko@willfind.org

Eduard Shuliak: eduard.shuliak@willfind.org

2. Include: Your full name, email address, and description of request

3. Specify: Which right you're exercising and your jurisdiction

4. Verification: We may request additional info to verify your identity

5. Response: We will respond within applicable legal timeframes

No Fee: We will not charge a fee for rights requests unless they are manifestly unfounded,

excessive, or repetitive (GDPR Art. 12(5)).

11. DATA SECURITY

11.1 Technical Measures

• Encryption: TLS/SSL for data in transit, AES-256 for data at rest

• Access Controls: Role-based access, multi-factor authentication for admin accounts

• Password Security: Bcrypt hashing with salt, no plaintext storage

• Secure Storage: Resumes stored in access-controlled Supabase buckets

• CSRF Protection: Anti-CSRF tokens for all state-changing requests

• XSS Prevention: Input validation and output encoding

11.2 Organizational Measures

• Employee Training: Regular security and privacy training

• Access Limitations: Employees access data only on a need-to-know basis

• Background Checks: For employees with access to sensitive data

• Vendor Management: Due diligence and contracts with all processors

• Incident Response: Documented procedures for security breaches

11.3 Data Breach Notification

In the event of a personal data breach:

• We will notify affected users within 72 hours (GDPR requirement)

• Notification will include: nature of breach, likely consequences, mitigation steps

• We will notify relevant supervisory authorities as required by law

• We will document all breaches per GDPR Article 33-34

11.4 Limitations

No method of transmission or storage is 100% secure. While we implement industry-standard security measures, we cannot guarantee absolute security. You are responsible for maintaining the confidentiality of your account credentials.

12. CHILDREN'S PRIVACY

Our Service is not intended for individuals under 16 years old (GDPR) / 13 years old (COPPA).

• We do not knowingly collect data from children

• If you are under 16 (or 13 in the US), do not use our Service

• If we learn we have collected data from a child, we will delete it immediately

• Parents/guardians: Contact

Mykyta Usatenko: mykyta.usatenko@willfind.org

Eduard Shuliak: eduard.shuliak@willfind.org

if you believe your

child has provided data

13. AUTOMATED DECISION-MAKING & PROFILING

We do NOT use automated decision-making or profiling that produces legal or similarly

significant effects (GDPR Article 22).

• Job Matching: Our job recommendation algorithm is informational only

• Search Results: Ranking is based on relevance, not automated decisions about you

• No AI Hiring Decisions: Employers make all hiring decisions manually

If we introduce automated decision-making in the future, we will:

• Notify you and obtain explicit consent

• Provide information about the logic involved

• Give you the right to contest decisions and request human review

14. CALIFORNIA "SHINE THE LIGHT" LAW

California residents may request information about disclosure of personal information to

third parties for direct marketing purposes (Cal. Civ. Code § 1798.83).

We do not share personal information with third parties for their direct marketing purposes.

15. NEVADA PRIVACY RIGHTS

Nevada residents have the right to opt-out of the sale of personal information (NRS 603A).

We do not sell personal information. If you wish to submit an opt-out request:

• Emails:

Mykyta Usatenko: mykyta.usatenko@willfind.org

Eduard Shuliak: eduard.shuliak@willfind.org

with subject "Nevada Opt-Out"

16. UPDATES TO THIS PRIVACY POLICY

We may update this Privacy Policy periodically to reflect:

• Changes in our data practices

• New legal requirements

• Service feature updates

• User feedback

Material Changes:

• Will be notified via email to registered users

• Prominent notice on our website for 30 days

• Updated "Last updated" date at the top

• For material changes requiring consent, we will obtain fresh consent

Your continued use after changes constitutes acceptance of the updated policy.

---

17. SUPERVISORY AUTHORITIES & COMPLAINTS

You have the right to lodge a complaint with a data protection authority:

European Union / EEA:

• Poland (UODO): https://uodo.gov.pl

• Your local EU supervisory authority: https://edpb.europa.eu/about-edpb/board/members_en

United Kingdom:

• Information Commissioner's Office (ICO): https://ico.org.uk

United States (California):

• California Attorney General: https://oag.ca.gov/privacy/ccpa

Brazil:

• Autoridade Nacional de Proteção de Dados (ANPD): https://www.gov.br/anpd

Canada:

• Office of the Privacy Commissioner: https://www.priv.gc.ca

---

18. CONTACT US

For any privacy-related questions, concerns, or rights requests:

📧 Email:

Mykyta Usatenko: mykyta.usatenko@willfind.org

Eduard Shuliak: eduard.shuliak@willfind.org

📬 Postal Address:

Refcruiter - Privacy Team

Mykyta Usatenko and Eduard Shuliak

Poland

⏱️ Response Time: Within 30 days (GDPR) / 45 days (CCPA)

📞 Alternative Contacts:

Mykyta Usatenko: mykyta.usatenko@willfind.org

Eduard Shuliak: eduard.shuliak@willfind.org

═══

END OF PRIVACY POLICY

═══

For Cookie Policy and Terms of Service, please see terms.txt or visit:

https://refcruiter.willfind.org/terms

https://refcruiter.willfind.org/cookie-settings

🔐 POLITYKA PRYWATNOŚCI – Refcruiter

Ostatnia aktualizacja: 6 lutego 2026

Data wejścia w życie: 6 lutego 2026

Niniejsza Polityka Prywatności opisuje, w jaki sposób Refcruiter („my”, „nas”, „nasz”) gromadzi, wykorzystuje, przetwarza oraz chroni dane osobowe użytkowników korzystających z naszej platformy ogłoszeń o pracę („Usługa”).

Polityka została opracowana zgodnie z obowiązującymi przepisami prawa, w szczególności:

Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 (RODO / GDPR)

Ustawą z dnia 10 maja 2018 r. o ochronie danych osobowych (Polska)

California Consumer Privacy Act (CCPA) / CPRA

Lei Geral de Proteção de Dados (LGPD – Brazylia)

PIPEDA (Kanada)

UK GDPR

Australian Privacy Act 1988

Innymi obowiązującymi przepisami o ochronie danych

1. ADMINISTRATOR DANYCH I DANE KONTAKTOWE

Administrator danych osobowych:

Mykyta Usatenko oraz Eduard Shuliak

działający jako Refcruiter

Siedziba: Polska

Strona internetowa: https://refcruiter.willfind.org

Kontakt w sprawach związanych z ochroną danych osobowych:

📧 mykyta.usatenko@willfind.org

📧 eduard.shuliak@willfind.org

Czas odpowiedzi:

do 30 dni (RODO)

do 45 dni (CCPA)

Administrator nie wyznaczył Inspektora Ochrony Danych (IOD), gdyż nie jest to wymagane na obecnym etapie działalności. W przypadku zmian zostaniesz poinformowany.

2. ZAKRES I DEFINICJE

Polityka dotyczy:

Kandydatów – osób przeglądających oferty pracy lub aplikujących

Pracodawców / Rekruterów – firm i osób publikujących oferty pracy

Odwiedzających stronę

Użytkowników niezarejestrowanych (Gości)

Dane osobowe – informacje umożliwiające identyfikację osoby fizycznej, bezpośrednio lub pośrednio.

3. DANE OSOBOWE, KTÓRE ZBIERAMY

3.1 Dane przekazywane bezpośrednio przez użytkownika

Dla wszystkich użytkowników:

dane konta (imię, nazwisko, e-mail, hasło – haszowane)

dane profilowe (stanowisko, lokalizacja)

dane kontaktowe (numer telefonu – opcjonalnie)

korespondencja z pomocą techniczną

Dla kandydatów:

CV / życiorys zawodowy

list motywacyjny

dane aplikacyjne

preferencje zawodowe

linki do profili (LinkedIn, GitHub, portfolio)

Dla pracodawców / rekruterów:

dane firmy

treść ogłoszeń

dane rozliczeniowe (NIP, adres)

płatności (obsługiwane wyłącznie przez Stripe)

3.2 Dane zbierane automatycznie

adres IP

typ przeglądarki i urządzenia

dane statystyczne dotyczące korzystania z serwisu

logi systemowe i zdarzenia bezpieczeństwa

pliki cookies (szczegóły w Polityce Cookies)

3.3 Dane od podmiotów trzecich

logowanie OAuth (Google, GitHub, LinkedIn)

Stripe – potwierdzenia płatności

usługi weryfikacji adresów e-mail

4. CELE PRZETWARZANIA DANYCH

4.1 Wykonanie umowy

obsługa kont użytkowników

publikacja ofert pracy

obsługa aplikacji kandydatów

komunikacja systemowa

realizacja płatności

4.2 Obowiązki prawne

księgowość i podatki

przeciwdziałanie nadużyciom

realizacja obowiązków ustawowych

4.3 Prawnie uzasadniony interes administratora

rozwój i optymalizacja Usługi

bezpieczeństwo systemów

obsługa klienta

analiza statystyczna

4.4 Zgoda użytkownika

marketing (newsletter)

cookies analityczne

integracje z mediami społecznościowymi

5. PODSTAWA PRAWNA PRZETWARZANIA (RODO)

art. 6 ust. 1 lit. b – wykonanie umowy

art. 6 ust. 1 lit. a – zgoda

art. 6 ust. 1 lit. f – prawnie uzasadniony interes

art. 6 ust. 1 lit. c – obowiązek prawny

Masz prawo sprzeciwu wobec przetwarzania danych na podstawie prawnie uzasadnionego interesu.

6. APLIKOWANIE NA OFERTY PRACY

Po złożeniu aplikacji:

Twoje CV trafia do bezpiecznego storage (Supabase)

pracodawca uzyskuje dostęp do dokumentów

pracodawca staje się niezależnym administratorem danych

Aplikacje gości przechowywane są przez 90 dni.

7. ODBIORCY DANYCH

pracodawcy (w przypadku aplikacji)

Supabase (hosting i storage)

Stripe (płatności)

dostawcy e-mail

organy publiczne (jeśli wymagane prawem)

❌ Nie sprzedajemy danych osobowych.

8. OKRES PRZECHOWYWANIA DANYCH

dane konta: do 90 dni po usunięciu konta

CV i aplikacje: 90 dni

dane księgowe: 7 lat

logi systemowe: 90 dni

dane statystyczne: zanonimizowane – bezterminowo

9. PRZEKAZYWANIE DANYCH POZA UE

Dane mogą być przetwarzane w UE oraz USA.

Stosujemy:

Standardowe Klauzule Umowne (SCC)

EU–US Data Privacy Framework

szyfrowanie danych

10. PRAWA UŻYTKOWNIKA

Zgodnie z RODO przysługuje Ci prawo do:

dostępu do danych

sprostowania

usunięcia

ograniczenia przetwarzania

przenoszenia danych

sprzeciwu

cofnięcia zgody

Wnioski należy kierować na:

📧 mykyta.usatenko@willfind.org

📧 eduard.shuliak@willfind.org

11. BEZPIECZEŃSTWO DANYCH

TLS / SSL

szyfrowanie AES-256

RBAC i MFA

hasła haszowane bcrypt

zabezpieczenia XSS / CSRF

12. DANE DZIECI

Usługa nie jest przeznaczona dla osób poniżej 16 lat.

Dane dzieci są usuwane niezwłocznie po wykryciu.

13. AUTOMATYCZNE DECYZJE

Nie stosujemy zautomatyzowanego podejmowania decyzji ani profilowania w rozumieniu art. 22 RODO.

14. ZMIANY POLITYKI

Zmiany będą komunikowane:

e-mailem

na stronie internetowej

15. ORGAN NADZORCZY

Masz prawo złożyć skargę do:

Prezes Urzędu Ochrony Danych Osobowych (UODO)

https://uodo.gov.pl

16. KONTAKT

📧 mykyta.usatenko@willfind.org

📧 eduard.shuliak@willfind.org

📍 Polska