

Complete Privacy Policy

Detailed privacy rules for WorkDirect's public website, application, recruitment functions, subscriptions, payments, technical logs and communications.

Last updated: 28 July 2026 | Effective: 28 July 2026

Important Platform Position

WorkDirect is a technology and recruitment platform, not a legal adviser, employer, embassy, immigration authority or guarantor. Promises made by users or third parties do not bind KEINN S.R.L. unless expressly accepted in a signed written agreement by an authorised representative. Mandatory legal rights and duties remain unaffected.

1. Introduction and Application

This Complete Privacy Policy explains how KEINN S.R.L. collects, uses, stores, discloses, protects and otherwise processes personal data in connection with WorkDirect and DirectWork.

It applies to workdirect.eu, app.workdirect.eu, directwork.eu, workdirect.org, workdirect.online, directwork.org, directwork.online, authorised subdomains, mobile or web interfaces, account areas, payment pages, communications and related recruitment or workforce services controlled by KEINN S.R.L. (together, the "Platform").

It covers candidates, jobseekers, workers, employers, recruiters, recruitment partners, business clients, suppliers, visitors, persons who contact us and persons whose data is lawfully submitted to the Platform.

The Platform may add, remove or change technical functions. A material change to personal-data processing will be reflected in an updated notice or an additional notice where required. This Policy does not automatically govern the independent activities of employers, recruiters, payment providers, government bodies or external websites.

2. Data Controller and Contact Details

Controller: KEINN S.R.L.

Registered office: Str. Dascălilor nr. 2, Sat Dancu, Comuna Holboca, Județul Iași, Romania

CUI: 51781577

Trade Register No.: J2025034047001

Privacy contact: info@workdirect.eu

KEINN S.R.L. determines the purposes and essential means of processing carried out through the Platform, except where another organisation acts as an independent controller or where a provider processes data on documented instructions.

3. Legal Framework and Principles

Processing is carried out under applicable European Union and Romanian law, including Regulation (EU) 2016/679 (GDPR), Romanian Law No. 190/2018 and Romanian Law No. 506/2004 where applicable.

We seek to apply lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity, confidentiality and accountability. Nothing in this Policy requires a person to waive a mandatory right.

4. Sources and Categories of Personal Data

We may receive information directly from the individual, through registration and account forms, uploads, applications, job posts, support or payment processes; from employers, recruiters, partners, representatives or references; from payment, hosting, verification or security providers; from public professional or company sources; and from technical use of the Platform.

Categories may include identity and contact details; account and authentication information; CV, skills, education, qualifications and employment history; job preferences, applications and interview information; photographs, videos and work samples; identity, residence, visa, work-permit or right-to-work material where necessary; employer and company information; job advertisements and staffing requests; declared representative identity and contact details; authority, permission, revocation and account-management records; communications and support history; billing, subscription and transaction information; complaint, fraud, dispute and compliance records; and technical and security data.

We do not request special-category or criminal-conviction information as a general registration condition. Such data should be submitted only where specifically required for a lawful and proportionate purpose and where an appropriate legal condition and safeguards exist.

5. Application Data, IP Addresses and Technical Logs

The application may automatically record IP address, date and time, account and session identifiers, login history, failed-login attempts, browser and version, device and operating system, language, screen or interface information, pages and actions, referrer, cookies or similar identifiers, diagnostic events, error or crash information, approximate location inferred from IP, network or ISP information, and security or anti-fraud signals.

Where technically detectable, signals may indicate VPN, proxy, Tor, automated access, abnormal traffic, duplicate accounts, credential abuse or other suspicious activity. Such signals are indicators only and may be incorrect. Access may be challenged or temporarily restricted where reasonably necessary to protect users, accounts or systems, and a person may request review of an incorrect restriction.

Routine access, page and session logs are normally retained for 30 to 90 days. Login, security, anti-fraud and diagnostic logs may be retained for up to 180 days. Logs connected to a specific incident, legal claim, fraud investigation, contractual dispute or authority request may be retained longer for the period reasonably necessary and lawful.

6. Purposes and Legal Bases

We process data to register and authenticate users; maintain accounts, representative permissions and access records; provide job-posting, search, application, candidate-profile and communication functions; support recruitment and workforce services; verify information where appropriate; manage employer and partner relationships; provide support; process subscriptions, invoices, refunds and payment status; prevent fraud, scams, unauthorised access and abuse; maintain, test and improve the Platform; comply with legal duties; and establish, exercise or defend legal claims.

Depending on the activity, the legal basis may be pre-contractual steps requested by the individual, performance of a contract, compliance with a legal obligation, legitimate interests, consent, or another basis allowed by law. Legitimate interests may include operating a reliable recruitment platform,

protecting accounts and candidate information, preventing fraud, maintaining accurate records, administering commercial relationships and resolving disputes.

Consent is used only where appropriate, such as optional marketing, non-essential cookies, selected public visibility, testimonials or particular sensitive processing. Consent may be withdrawn at any time without affecting earlier lawful processing.

7. Accounts, Candidate Profiles and Applications

A person may need to provide mandatory information to open an account, publish a job, create a candidate profile, purchase a service, apply for an opportunity or complete verification. Failure to provide required information may prevent or delay the requested service.

Candidate profiles may be private, visible to selected recipients, searchable by registered employers, or publicly visible only where the feature and user choice allow it. Candidates should use available controls carefully and should not place passports, full home addresses, passwords, financial credentials or unnecessary sensitive information in public or employer-visible fields.

Candidate information may be disclosed to an employer, its declared account Representative, or an authorised recruitment partner when a candidate applies, requests an introduction, enables visibility, selects a recipient or uses a service that reasonably requires the disclosure. We seek to limit disclosure to information relevant to recruitment, verification, employment, onboarding or a related lawful purpose.

8. Employers, Recruiters and Publishers

An employer, recruiter, agency, representative or other publisher is responsible for ensuring that it is lawfully established where required, authorised to act, and entitled to publish or request the relevant information.

The publisher is solely responsible for the truth, legality, completeness and accuracy of company details, job availability, job descriptions, salary, deductions, fees, working time, location, accommodation, transport, insurance, visa or work-permit support, employment terms, start dates, refund statements and every other representation or commitment it makes.

Employers and recruiters receiving candidate information may act as independent controllers. They must establish their own legal basis, provide any required privacy information, protect the data, restrict use to legitimate recruitment or employment purposes, respect rights, prevent unauthorised copying or resale and delete information when no longer lawfully needed.

Employers may pay for subscriptions, job-posting or candidate-search functionality. Such payment is for a professional service and does not transfer ownership of personal data or permit resale, scraping, unrelated marketing, identity trading or unauthorised database creation.

9. Third-Party Representatives and Account Management

An employer or recruiter (the "Account Holder") may authorise an employee, consultant, recruitment agency, contractor, administrator, representative or other third party (a "Representative") to assist with operation of its WorkDirect account. Before access is granted, the Account Holder must declare and authorise the Representative through Dashboard > Account Management where that function is available and must keep the information accurate and current.

Where WorkDirect provides separate representative credentials or permission controls, the Account Holder must use those controls rather than unnecessarily sharing its primary password. The Account Holder is responsible for selecting and verifying the Representative, defining permissions, supervising activity, protecting credentials, reviewing actions, ensuring lawful and confidential use of candidate data, and revoking access immediately when authority ends or misuse is suspected.

Unless unauthorised access is reported promptly, actions performed through the account by a declared Representative may be treated as actions authorised by the Account Holder. This includes publishing or editing vacancies, searching or viewing candidate profiles, downloading or receiving candidate information, contacting candidates, arranging interviews, making offers, describing salary or working conditions, requesting documents, sending payment or refund instructions, purchasing services, accepting Platform terms and changing account settings.

The Account Holder and Representative may use candidate information only for legitimate and lawful recruitment, employment, verification or related purposes. They must not sell, redistribute or scrape candidate data; build an unauthorised external database; disclose information without lawful authority; permit access by another undeclared person; retain data longer than lawfully necessary; or use information for unrelated marketing, discrimination, harassment, fraud or deception.

WorkDirect does not employ, supervise, recommend, certify or guarantee a Representative merely because the Representative is declared in Account Management or uses the Platform. Any vacancy, message, offer, promise, assurance, payment instruction, refund statement, employment condition, immigration statement or other commitment made by the Account Holder or Representative is made on their own behalf. It is not a statement or commitment of KEINN S.R.L. and does not bind KEINN S.R.L. unless expressly accepted in a separate signed written agreement by an authorised KEINN S.R.L. representative.

WorkDirect may request evidence of authority, restrict permissions, preserve relevant account and technical records, remove misleading content, suspend or terminate access, notify affected parties or cooperate with competent authorities where undeclared, suspicious, misleading or unlawful account management is detected. The Account Holder remains responsible to WorkDirect for the acts and omissions of its authorised Representative. Nothing in this section excludes liability or statutory duties that cannot lawfully be excluded or responsibility arising directly from KEINN S.R.L.'s own proven acts or omissions.

For account administration, security, privacy, fraud prevention and dispute handling, WorkDirect may process the Representative's identity and contact details, authority and permission records, authorisation and revocation dates, account actions, access times, IP addresses, device or session information, messages and related security events. Routine access and session logs are normally retained for 30 to 90 days, while login, security, anti-fraud and incident-related logs may be retained for up to 180 days, subject to longer retention where a specific legal claim, investigation, dispute or binding legal obligation requires it.

10. Verification and Its Limits

WorkDirect may use reasonable registration, identity, document, company, fraud or compliance checks. It may request supporting information, restrict suspicious accounts, remove posts, seek clarification or report suspected illegality where appropriate.

WorkDirect cannot independently inspect every workplace, bank account, contract, government record, recruiter relationship, financial condition, accommodation, immigration process or statement. It does not guarantee that every user is honest, every document is genuine, every vacancy remains available, every employer will perform, every candidate is suitable, every payment will be recovered, or any visa, permit, interview, placement or employment outcome will occur.

A company registration number, account approval, identity check, published post, verification label, payment, communication through the Platform or absence of a warning does not constitute a guarantee, insurance, warranty or endorsement by KEINN S.R.L.

11. Platform Role, No Professional Advice and Third-Party Promises

WorkDirect is a technology and recruitment platform. Unless KEINN S.R.L. expressly assumes a different role in a separate written agreement signed by an authorised representative, WorkDirect is not an

employer, employee, immigration authority, embassy, consulate, government representative, law firm, tax adviser, financial adviser, insurer, guarantor, fiduciary, escrow service or party to a contract between users or third parties.

Information on the Platform is general operational or recruitment information. It is not legal, immigration, tax, financial, medical or other regulated professional advice. Users should obtain advice from a qualified professional or competent authority where appropriate.

No offer, salary statement, job guarantee, visa assurance, relocation promise, accommodation commitment, fee request, payment instruction, reimbursement or refund promise, contract term or other representation made by an employer, recruiter, candidate, agent, partner or third person—inside or outside the Platform, including by email, telephone, messaging application, social media or in-person meeting—creates an obligation for KEINN S.R.L. unless expressly accepted in a separate signed written agreement by an authorised KEINN S.R.L. representative.

Users must independently verify material terms before signing, resigning from work, travelling, paying money, releasing original documents or relying on a statement. Suspicious conduct should be reported promptly. Nothing in this section excludes liability or statutory duties that cannot lawfully be excluded, including KEINN S.R.L.'s duties under data-protection law.

12. Identity, Work-Authorisation and Verification Material

Where necessary for a particular service or lawful recruitment process, we may process passports, national identity cards, residence permits, visas, work permits, selfies, photographs, videos, signatures or related verification material.

Access should be limited to authorised persons with a legitimate need. We may obscure unnecessary fields, apply watermarks, limit download rights, store materials separately, log access, reject altered or unclear documents and delete complete copies when no longer necessary while retaining a limited verification record.

An ordinary photograph, video or voice recording is not treated as biometric data merely because it contains a face or voice. If technology is introduced to process biometric data for unique identification, a specific notice, legal basis, safeguards and any required impact assessment or explicit consent will be addressed separately.

13. Payments, Subscriptions and Financial Data

WorkDirect may process billing name and address, company or tax details, plan, amount, currency, invoice, transaction identifier, payment status, subscription status, refund status, chargeback information and limited payment-method information received from a payment provider.

Where Stripe or another hosted payment provider is used, complete card numbers and card security codes are generally entered directly into the provider's environment and are not intentionally stored by WorkDirect. The payment provider processes information under its own privacy terms and regulatory obligations.

Payments, renewals, cancellation, refund eligibility, payment disputes and service access are also governed by the applicable Terms of Service and Payment Terms.

14. Recipients and Service Providers

Personal data may be shared, where necessary and lawful, with selected employers and prospective employers; their declared account Representatives; recruitment agencies and authorised partners; hosting, cloud, database, storage, development, maintenance, cybersecurity, email, SMS, communications, customer-support, analytics, error-monitoring, translation, document or video providers; payment processors; accountants, auditors, lawyers, insurers and advisers; and competent courts, police, tax, labour, immigration, consumer-protection or data-protection authorities.

Processors must be subject to documented obligations appropriate to their role. Independent controllers determine their own purposes and means and are responsible for their own compliance. KEINN S.R.L. remains responsible for its own disclosure decisions.

15. International Transfers

Recruitment and technical services may involve access from or transfer to countries outside Romania or the European Economic Area. International recruitment does not justify unrestricted disclosure, and data should be limited to what is reasonably necessary.

Where required, a transfer will rely on an adequacy decision, European Commission Standard Contractual Clauses, another recognised safeguard or a lawful derogation for a specific situation. Additional contractual, organisational or technical safeguards may be used where appropriate.

16. Cookies, Analytics and Marketing

The Platform may use cookies, local storage, session storage and similar technologies for authentication, security, fraud prevention, user settings, language, session continuity, performance, diagnostics, analytics and marketing.

Strictly necessary technologies may be used without consent where legally permitted. Non-essential analytics, advertising or marketing technologies will be used only after consent where required. Users should be able to accept, reject, customise and later change non-essential choices.

Service communications may concern accounts, applications, security, verification, payments, contracts, legal notices or operation of the Platform. Marketing may be sent only where legally permitted. A person may unsubscribe or object to direct marketing at any time, and limited suppression data may be retained to respect the choice.

17. Retention

We retain data only for as long as reasonably necessary for the relevant service, recruitment, contractual, accounting, legal, security, fraud-prevention or dispute purpose.

Routine technical and session logs: normally 30 to 90 days. Login, security, anti-fraud and diagnostic logs: up to 180 days, subject to longer incident-specific retention where justified.

Incomplete registrations and abandoned drafts: normally up to 90 days. Active account and profile information: while active and for a reasonable closure period. Inactive candidate accounts: may be reviewed, restricted, anonymised or deleted after approximately 24 months without meaningful activity.

Candidate profiles, applications and recruitment communications: normally up to three years after the last meaningful activity. Identity documents, selfies and verification videos: the shortest practical period, normally no longer than 12 months after verification or completion of the relevant process unless an active recruitment, immigration, fraud, dispute or legal matter requires longer retention.

Routine support communications: normally up to 24 months after closure. Employer, business and representative authorisation records: for the relationship or period of authority and normally up to three years afterwards where reasonably necessary for administration, security, contractual enforcement or disputes, unless a longer or shorter period is required. Invoices and accounting records: for the statutory period under Romanian law. Complaints, fraud, security incidents and legal claims: until resolution and for the applicable limitation period.

Deleted data may remain temporarily in secured backups until overwritten under the backup cycle. At the end of the relevant period, data will be securely deleted, irreversibly anonymised or restricted where continued retention is legally required.

18. Security and Technical Providers

KEINN S.R.L. operates WorkDirect but is not the original developer of every software component and does not claim to be a specialist cybersecurity company. The Platform may depend on independent developers, hosting companies, infrastructure providers, payment processors, communication vendors and other technical providers. Each provider is responsible for its services within its contractual and legal role.

KEINN S.R.L. remains responsible for obligations that apply to it as controller and for selecting and managing providers appropriately. Measures within its practical control may include encrypted transmission, password hashing, access restrictions, role-based permissions, administrator controls, available multi-factor authentication, logging, backups, updates, vulnerability remediation, confidentiality requirements, provider review and incident procedures. The precise controls may vary as technology and providers change.

No online service, device, network or storage system can be guaranteed to be completely secure. Users must use unique passwords, protect their email and devices, avoid sharing credentials, log out of shared devices and report suspected compromise promptly.

19. Personal-Data Breaches

If KEINN S.R.L. becomes aware of a suspected personal-data breach affecting data under its responsibility, it will assess the nature, scope, likely consequences and risks; preserve appropriate records; coordinate with the relevant developer, host or service provider; and take reasonable containment and remediation steps within its control.

Where legally required, KEINN S.R.L. will notify the competent supervisory authority without undue delay and, where feasible, within the statutory period. Affected individuals will be informed where the breach is likely to result in a high risk to their rights and freedoms, unless a lawful exception applies. Notification may be limited or delayed where required by law or necessary to avoid compromising a legitimate investigation.

20. Automated Tools and Artificial Intelligence

Automated or artificial-intelligence tools may assist with search, ranking, matching, translation, classification, summarisation, duplicate detection, fraud detection, support, analytics or security. Outputs may be incomplete or incorrect and should not be treated as unquestionable.

Unless separately disclosed, WorkDirect does not make a decision based solely on automated processing that produces legal or similarly significant effects. Where such processing is introduced, affected persons will receive the information and rights required by law, including human intervention where applicable.

21. Children

The Platform is intended primarily for adults. A person must ordinarily be at least 18 years old to create an independent candidate or employer account.

Where a lawful programme involves a person under 18, processing will occur only with the legal basis, authorisation and safeguards required by law. If information concerning a child is submitted without lawful authority, the account or data may be restricted or deleted.

22. Data-Subject Rights

Subject to legal conditions and exceptions, individuals may request information and access; correction; deletion; restriction; portability of eligible data; objection to processing based on legitimate interests;

unconditional objection to direct marketing; withdrawal of consent; and rights concerning qualifying automated decisions.

Requests should be sent to info@workdirect.eu and identify the person, account and request clearly. We may request proportionate verification and will not routinely require an identity-document copy where a less intrusive method is sufficient.

Requests are normally answered within one month. The period may be extended by up to two additional months where permitted because of complexity or volume, and the person will be informed. Requests are normally free, but a reasonable fee may be charged or action refused where a request is manifestly unfounded or excessive as permitted by law.

23. Account Closure and Deletion

A user may request account closure through available settings or by contacting the privacy email. Closure does not require immediate deletion of every record.

Limited data may be retained where necessary for accounting, tax, fraud prevention, contractual enforcement, disputes, legal claims, suppression preferences, authority requests or another lawful purpose. Where complete deletion is not possible, information will be restricted to the permitted purpose.

24. External Services and Independent Controllers

The Platform may link to employer websites, recruitment partners, payment services, maps, government portals, social networks, messaging services and other external resources. Their presence does not guarantee their security, accuracy or conduct.

External organisations may process data as independent controllers under their own privacy notices. Users should review those notices before providing information. WorkDirect is not responsible for independent processing that it does not determine or control, but it remains responsible for its own decisions to disclose data.

25. Complaints and Supervisory Authority

Privacy questions, rights requests, security reports and complaints may be sent to info@workdirect.eu.

Individuals may also complain to the Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP), 28-30 General Gheorghe Magheru Boulevard, District 1, Bucharest, Romania, or another competent supervisory authority where applicable.

Contacting WorkDirect first may allow a concern to be resolved promptly, but it is not a condition for exercising the right to complain to an authority.

26. Related Documents, Conflicts and Changes

This Policy should be read together with the WorkDirect Terms of Service, Payment Terms, Cookie Policy, Anti-Scam & Candidate Protection Policy, Recruitment Process & Cooperation Policy, Legal Information and any specific notice presented for a feature or service.

If documents conflict on the processing of personal data, this Complete Privacy Policy applies to the privacy issue unless mandatory law or a more specific lawful notice requires otherwise. Commercial, payment, recruitment and user-conduct matters remain governed by the relevant terms.

We may update this Policy for changes in law, services, providers, processing, security or business operations. The revised date will be displayed. Material changes may be notified by email, account message, website banner or another appropriate method. Continued use will not substitute for new consent where consent is legally required.

27. Final Contact Information

KEINN S.R.L. — Operator of WorkDirect

Registered office: Str. Dascălilor nr. 2, Sat Dancu, Comuna Holboca, Județul Iași, Romania

CUI: 51781577 | Trade Register No.: J2025034047001

Privacy and security contact: info@workdirect.eu

Users should verify that communications claiming to represent WorkDirect use an official authorised domain. Suspected phishing, impersonation or misuse of the WorkDirect name should be reported promptly.