Privacy Policy

How we collect, use, and protect your personal data.

Table of Contents

Our Commitment to Privacy

Wizard Software Solutions Ltd is committed to protecting your privacy and handling your data with transparency. This Privacy Policy explains how we collect, use, disclose, and safeguard your information when you use our platform. We are fully compliant with GDPR, UK Data Protection Act 2018, the Brazilian General Data Protection Law (LGPD), the Japanese Act on the Protection of Personal Information (APPI), India's Digital Personal Data Protection Act 2023 (DPDP Act), US state privacy laws (including the CCPA/CPRA, VCDPA, CPA, CTDPA, UCPA, TDPSA, OCPA, and MCDPA), and other applicable privacy regulations worldwide.

1. Information We Collect

1.1 Information You Provide

We collect information that you voluntarily provide to us when you:

- **Register an account:** Company name, subdomain, administrator name, email address, password
- **Use our service:** Candidate data (CVs, contact information, skills, work history), job postings, company information, notes, and communications
- **Contact us:** Name, email address, phone number, and message content
- **Subscribe:** Billing information, payment card details (processed securely by our payment processor)
- **Provide feedback:** Survey responses, feature requests, bug reports

1.2 Automatically Collected Information

When you access our service, we automatically collect certain information:

- **Log data:** IP address, browser type, operating system, pages visited, time spent on pages, access times
- **Device information:** Device type, unique device identifiers, mobile network information
- **Cookies and tracking:** We use cookies and similar technologies to track activity and store certain information
- **Usage data:** Features used, actions taken, time spent in the application, search queries
- **Performance data:** Page load times, response times, system errors

1.3 Candidate Data

When you upload candidate CVs or enter candidate information, you are responsible for ensuring you have the legal right to process this data. As the data controller, you must obtain appropriate consent from candidates. Candidate data may include:

- Personal information (names, contact details, addresses, date of birth)
- Professional information (work history, education, skills, qualifications)
- CV documents and attachments
- Application materials and correspondence
- Interview notes and assessments
- Right-to-work documentation

We act as a data processor for candidate data, and you act as the data controller. You are responsible for ensuring compliance with data protection laws when processing candidate data through our platform.

2. How We Use Your Information

We use the collected information for various purposes:

- **Provide and maintain our service:** Enable core functionality, process registrations, manage accounts
- **Process AI features:** Parse CVs, match candidates to jobs, generate job descriptions using AI/ML algorithms
- **Communications:** Send service-related emails, notifications, updates, and support responses
- **Billing and payments:** Process subscriptions, send invoices, manage billing, prevent payment fraud
- **Improve our service:** Analyse usage patterns, develop new features, enhance user experience, conduct A/B testing
- **Security:** Monitor for suspicious activity, prevent fraud, detect security incidents, enforce our terms
- **Legal compliance:** Comply with legal obligations and respond to legal requests
- **Marketing:** Send promotional emails about new features and services (you can opt out at any time)
- **Customer support:** Respond to enquiries, troubleshoot issues, provide technical assistance
- **Research and development:** Develop new products and services, improve existing features

3. Legal Basis for Processing (GDPR)

Under the General Data Protection Regulation (GDPR) and UK GDPR, we process your personal data based on the following legal grounds:

- **Contract performance:** Processing necessary to provide our services under our agreement with you (Article 6(1)(b) GDPR)
- **Legitimate interests:** Improving our service, preventing fraud, ensuring security, conducting analytics (Article 6(1)(f) GDPR)
- **Consent:** Where you have given explicit consent for specific processing activities such as marketing communications (Article 6(1)(a) GDPR)
- **Legal obligation:** Compliance with applicable laws and regulations, tax obligations, responding to legal requests (Article 6(1)(c) GDPR)

For candidate data where you are the controller, you must ensure you have an appropriate legal basis for processing, which may include:

- Consent from the candidate
- Performance of a contract with the candidate
- Legal obligations (e.g., right-to-work checks)
- Legitimate interests (e.g., business operations)

4. Data Sharing and Disclosure

4.1 Service Providers

We may share your information with trusted third-party service providers who perform services on our behalf:

- **Cloud hosting:** For secure data storage and infrastructure (AWS, Google Cloud, or similar providers)
- **Payment processors:** To process subscription payments securely (Stripe, PayPal, or similar providers)
- **Email services:** To send transactional and marketing emails (SendGrid, Mailgun, or similar providers)
- **Website analytics:** Visitor analytics on this marketing site are first-party — no third-party analytics service is used. Pageviews are recorded directly by us with no cookies, no fingerprinting, and IP addresses truncated before storage. See section 8 for details.
- **AI services:** To power CV parsing and candidate matching features
- **Customer support tools:** To provide efficient customer support
- **Security services:** To monitor and protect against security threats

These service providers are contractually obligated to protect your data, use it only for the purposes we specify, and comply with applicable data protection laws. We conduct due diligence on all service providers to ensure they maintain appropriate security measures.

4.2 Job Board Integrations

When you choose to post jobs to external job boards (Indeed, Reed, Totaljobs, LinkedIn, etc.), job information is shared with those platforms according to their privacy policies. We recommend reviewing the privacy policies of these third-party platforms.

4.3 Legal Requirements

We may disclose your information if required by law or in response to valid requests by public authorities, including:

- Court orders and subpoenas
- Law enforcement or government agency requests
- Tax authorities
- Regulatory bodies
- Legal proceedings and litigation

We will notify you of such requests unless prohibited by law.

4.4 Business Transfers, Corporate Restructuring, and Insolvency

Personal data is considered a business asset. Your information may therefore be disclosed to or

transferred to a third party if Wizard Software Solutions Ltd, or any of its assets or business units, is involved in any of the following corporate transactions:

- A merger, consolidation, or restructuring (including intra-group reorganisations)
- An acquisition or change of control of the company or any controlling interest in it
- The sale, assignment, or transfer of all or substantially all of our assets, or of a relevant business unit, product line, or customer book
- A joint venture, spin-off, divestiture, or other transaction affecting the entity that controls your personal data
- Insolvency proceedings of any kind, including administration, receivership, liquidation, or bankruptcy, and any transfer to a trustee, administrator, liquidator, or comparable office-holder
- Equity or debt financing, refinancing, securitisation, or similar transactions where access to personal data is required to evaluate or perfect the transaction
- Due diligence in connection with any of the above — in which case disclosure to potential counterparties, their advisers, and other relevant professionals is limited to what is reasonably necessary to evaluate the transaction and is subject to written confidentiality undertakings

Where any such transfer takes place, the following safeguards apply:

- **Continuity of protection:** the receiving party will be bound, by contract or by operation of law, to handle your personal data in accordance with this Privacy Policy and applicable data protection law (UK GDPR, EU GDPR, the LGPD, and applicable US state privacy laws) until any superseding policy is communicated to you.
- **Notice:** we will notify you of the transfer either by email to the address associated with your account or by a prominent notice on this website, in advance of the transfer where practicable, and otherwise as soon as reasonably possible afterwards.
- **Material changes:** if the receiving party intends to process your personal data for materially different purposes or under a different privacy policy, we (or the receiving party) will notify you, and, where required by law, obtain your consent before that new processing begins.
- **Continuity of your rights:** the rights described in this Privacy Policy (including under GDPR, UK GDPR, the LGPD, and US state privacy laws) continue to apply, and you may exercise them — including the right to deletion — against the receiving party in the same way that you may exercise them against us today.
- **Right to delete before transfer:** where legally permissible and operationally feasible, you may request deletion of your personal data prior to the completion of the transfer, subject to our existing retention obligations described in Section 6.

Treatment under specific privacy laws:

- **UK / EU (GDPR):** any transfer to a successor or affiliated entity will rely on the legal bases set out in Section 3 (typically legitimate interests for the orderly transfer of a business, or contract performance where the successor takes over our agreement with you); where personal data leaves the UK or EEA, the safeguards described in Section 9 (International Data Transfers) apply.
- **Brazil (LGPD):** for data subjects in Brazil, the receiving party assumes the controller obligations under the LGPD upon completion of the transfer; such transfers form part of the regular

conduct of business and rely on Articles 7(II) and 7(IX) (compliance with legal obligation and legitimate interest, respectively) rather than on fresh consent, unless consent is the original legal basis for the specific processing in question.

- **United States:** the transfer of personal information as an asset of a business that is the subject of a merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of our business is an exempt transaction under the CCPA / CPRA, VCDPA, CPA, CTDPA, UCPA, TDPSA, OCPA, MCDPA, and comparable US state privacy laws, and is not a "sale" or "share" for the purposes of those laws.

4.5 We Never Sell Your Data

No Data Sales

We do not and will never sell, rent, or trade your personal information to third parties for their marketing purposes. Your data is yours, and we respect that.

5. Data Security

We implement robust, industry-leading security measures to protect your information:

- **Encryption:** All data is encrypted in transit using TLS 1.3 and at rest using AES-256 encryption
- **Access controls:** Role-based access control (RBAC), multi-factor authentication (MFA) for administrators, principle of least privilege
- **Multi-tenant isolation:** Each customer's data is completely isolated in separate database schemas
- **Regular backups:** Automated daily backups with point-in-time recovery capabilities
- **Security monitoring:** 24/7 security monitoring, intrusion detection, and automated alerting
- **Penetration testing:** Annual third-party security audits and vulnerability assessments
- **Compliance:** GDPR compliant, working towards ISO 27001 certification
- **Incident response:** Documented incident response procedures and breach notification protocols
- **Employee security:** Background checks, security awareness training, signed confidentiality agreements
- **Physical security:** Data centres with physical access controls, surveillance, and environmental monitoring
- **Secure development:** Security testing in development lifecycle, code reviews, dependency scanning

However, no method of transmission over the Internet or electronic storage is 100% secure. While we strive to use commercially acceptable means to protect your data and maintain industry-leading security practices, we cannot guarantee absolute security.

6. Data Retention

We retain your information only for as long as necessary to provide our services and comply with legal obligations:

- **Active accounts:** Data is retained for the duration of your subscription
- **Cancelled accounts:** Data is retained for 30 days after cancellation, allowing you to reactivate your account
- **Deleted accounts:** After 30 days of cancellation, all customer data is permanently deleted from our production systems
- **Backups:** Deleted data may persist in encrypted backups for up to 90 days before permanent removal
- **Legal requirements:** Some data (e.g., billing records, audit logs) may be retained for up to 7 years to comply with tax and legal obligations
- **Anonymised data:** We may retain anonymised, aggregated data indefinitely for analytics and research purposes

You can request early deletion of your data by contacting legal@wizardapplication.com, subject to our legal obligations to retain certain records.

7. Your Rights Under GDPR

If you are in the European Economic Area (EEA) or the United Kingdom, you have the following data protection rights under GDPR and UK GDPR:

- **Right to access (Article 15):** Request copies of your personal data. We will provide this information free of charge within one month.
- **Right to rectification (Article 16):** Request correction of inaccurate or incomplete data
- **Right to erasure (Article 17):** Request deletion of your personal data ("right to be forgotten"), subject to certain exceptions
- **Right to restrict processing (Article 18):** Request that we limit how we use your data in certain circumstances
- **Right to data portability (Article 20):** Receive your data in a structured, commonly used, machine-readable format (CSV, JSON, XML)
- **Right to object (Article 21):** Object to our processing of your personal data, particularly for direct marketing
- **Right to withdraw consent (Article 7):** Withdraw consent at any time where we rely on consent to process your data
- **Right to lodge a complaint (Article 77):** File a complaint with your local data protection authority (Information Commissioner's Office in the UK)
- **Right to not be subject to automated decision-making (Article 22):** Not be subject to decisions based solely on automated processing

To exercise these rights, please contact us at legal@wizardapplication.com. We will respond to your

request within one month. If we need more time, we will inform you and explain why.

8. Cookies, Tracking and Website Analytics

We use cookies and similar storage on our service. Separately, this marketing website uses first-party analytics with no cookies, no third-party services, and no cross-site tracking. The two are described below.

8.1 Types of Cookies We Use (in the application)

- **Essential cookies:** Required for the service to function properly (authentication, security, session management). These cannot be disabled.
- **Preference cookies:** Remember your settings, language preferences, and customisation options.
- **Analytics cookies (in-app only):** Help us understand how customers interact with the application after sign-in. These are first-party and limited to the authenticated product.

We do not use third-party advertising or marketing cookies on this website or in the application.

8.2 Cookie Duration

- **Session cookies:** Deleted when you close your browser.
- **Persistent cookies:** Remain on your device for a set period or until manually deleted.

8.3 Managing Cookies

You can instruct your browser to refuse all cookies or indicate when a cookie is being sent. However, if you do not accept cookies, some parts of our service may not function properly. You can manage cookie preferences through:

- Your browser settings (Chrome, Firefox, Safari, Edge).
- Browser extensions for cookie management.

8.4 Website Analytics (this marketing site)

We operate first-party analytics on our website (wizardapplication.com and its localised paths) so we can see which pages are popular, where visitors arrive from, and how the site performs. This is built and hosted entirely by us — no Google Analytics, no third-party tracker, and no data leaves our infrastructure.

For each page request we record:

- The path you requested and the resolved language.
- The HTTP referrer (so we can attribute traffic sources) — never stored when you navigate

within our own site.

- Browser family, device type, and HTTP response status.
- Country code derived from your IP at the network edge.
- A truncated IP address (last octet zeroed for IPv4, last 80 bits zeroed for IPv6) — we never store the full IP.
- A daily-rotating session hash derived from your truncated IP, browser identifier, the date, and a server-side secret. This hash cannot identify you and changes every day.

From the browser, an additional first-party signal records how long you stayed on a page, your maximum scroll depth, and any clicks on outbound links. This signal is sent via navigator.sendBeacon when you leave the page. It uses no cookies and no client-side identifier.

Opt-out: the client-side signal automatically respects the *Do Not Track* and *Global Privacy Control* browser headers — if either is set, no client-side beacon is sent. The server-side pageview log still runs, but the data we keep about it is the truncated, hashed information described above.

Legal basis (UK GDPR / GDPR Art. 6(1)(f)): our legitimate interest in measuring traffic and improving the website, balanced against the privacy-protective design of the system. Because the website analytics use no cookies and no client-side identifiers, prior consent under PECR / ePrivacy is not required.

8.5 Form Spam Protection

Our public forms (*contact*, *register*, *feature requests*) are protected by a first-party anti-spam check that runs entirely on our infrastructure. It combines an invisible honeypot field, a server-signed timestamp, and per-IP rate limiting. No third-party CAPTCHA, no Google reCAPTCHA, no Cloudflare Turnstile.

9. International Data Transfers

Wizard Software Solutions Ltd is a UK-registered company operating a cloud-based platform. Our service runs on Amazon Web Services (AWS), which provides our compute, storage, networking, and content-delivery infrastructure across globally distributed regions. AWS auto-scaling provisions capacity in the regions appropriate to demand, which means your data may, at times, transit through or be temporarily processed in AWS regions outside the United Kingdom or European Economic Area (EEA) — for example, when static content is served via globally distributed edge caches, when backups replicate to a secondary region for resilience, or when the service auto-scales to handle surges in traffic. Persistent customer records (your account data, candidate data, documents, and other records you create within the platform) are stored in our primary UK / EEA regions.

Where personal data is transferred outside the UK or EEA, we rely on the following lawful safeguards under UK GDPR and EU GDPR:

- **Adequacy decisions:** Transfers to countries that the UK Government and/or the European Commission have determined provide an adequate level of data protection.

- **Standard Contractual Clauses (SCCs) and the UK Addendum:** European Commission–approved SCCs together with the UK ICO's International Data Transfer Addendum are in place with AWS and with every other sub-processor that may handle personal data outside the UK / EEA.
- **AWS Data Processing Addendum:** We have entered into AWS's Data Processing Addendum, which incorporates the SCCs and the UK Addendum, and which obligates AWS to apply equivalent safeguards across all of the regions in which our workloads run.
- **Encryption in transit and at rest:** All personal data is encrypted in transit using TLS 1.3, and at rest using AES-256, in every region where it is stored or processed.
- **Data minimisation:** The data that may transit globally (e.g. via CDN edge caches) is limited to what is required to serve the requested content; we do not replicate complete customer datasets to non-EEA regions for any other purpose.

You can request the specific safeguards in place — including a current list of AWS regions where your data may be stored or processed, and our current sub-processor list — by contacting legal@wizardapplication.com.

10. Children's Privacy

Our service is not intended for individuals under the age of 16. We do not knowingly collect personal information from children under 16. If you are a parent or guardian and believe your child has provided us with personal information, please contact us immediately at legal@wizardapplication.com.

If we become aware that we have collected personal data from a child under 16 without verification of parental consent, we will take steps to delete that information from our servers as quickly as possible.

11. Third-Party Links

Our service may contain links to third-party websites, job boards, and services. We are not responsible for the privacy practices or content of these external sites. We encourage you to read the privacy policy of every website you visit.

When you click on a third-party link, you will be directed to that third party's site. We have no control over and assume no responsibility for the content, privacy policies, or practices of any third-party sites or services.

12. Do Not Track Signals

We do not currently respond to "Do Not Track" (DNT) signals from web browsers, as there is no universally accepted standard for how to respond to such signals. We may implement DNT support in the future if industry standards develop.

13. US State Privacy Rights

If you are a resident of a US state with a comprehensive consumer privacy law, you have specific rights regarding your personal information. We extend the following rights to residents of all US states that have enacted such laws, including California, Virginia, Colorado, Connecticut, Utah, Texas, Oregon, Montana, Iowa, Delaware, New Hampshire, New Jersey, Tennessee, Nebraska, Maryland, Minnesota, and Indiana:

- **Right to know / access:** Confirm whether we process your personal information and request a copy of the data we hold about you
- **Right to delete:** Request deletion of personal information we have collected from you, subject to certain legal exceptions
- **Right to correct:** Request correction of inaccurate personal information we maintain about you
- **Right to data portability:** Receive your personal information in a portable, readily usable format where technically feasible
- **Right to opt-out:** Opt out of (a) the sale of personal information, (b) the sharing of personal information for cross-context behavioural advertising, and (c) profiling in furtherance of decisions that produce legal or similarly significant effects
- **Right to limit use of sensitive personal information:** Restrict our use and disclosure of sensitive personal information to purposes necessary to provide the requested service
- **Right to non-discrimination:** Not receive discriminatory treatment for exercising any of these rights
- **Right to appeal:** If we deny your request, you may appeal our decision; certain state laws (including Virginia's VCDPA, Colorado's CPA, Connecticut's CTDPA, and Texas' TDPSA) require us to respond to appeals within a defined period

13.1 Specific State Laws

The following state laws apply to our processing of personal information:

- **California:** California Consumer Privacy Act (CCPA) and California Privacy Rights Act (CPRA)
- **Virginia:** Virginia Consumer Data Protection Act (VCDPA)
- **Colorado:** Colorado Privacy Act (CPA)
- **Connecticut:** Connecticut Data Privacy Act (CTDPA)
- **Utah:** Utah Consumer Privacy Act (UCPA)
- **Texas:** Texas Data Privacy and Security Act (TDPSA)
- **Oregon:** Oregon Consumer Privacy Act (OCPA)
- **Montana:** Montana Consumer Data Privacy Act (MCDPA)
- **Other states:** Equivalent rights are extended to residents of Iowa, Delaware, New Hampshire, New Jersey, Tennessee, Nebraska, Maryland, Minnesota, and Indiana under their respective comprehensive privacy statutes

13.2 How to Exercise Your Rights

You can exercise any of these rights through either of two designated methods:

- Email us at legal@wizardapplication.com.
- Submit a privacy rights request via our contact form.

We will verify your identity before processing your request and respond within the timeframes required by your state's law (generally 45 days, extendable by an additional 45 days where reasonably necessary). You may designate an authorised agent to act on your behalf, and we will not charge a fee for the first such request in a twelve-month period.

13.3 Sale and Sharing of Personal Information

We do not sell personal information for monetary consideration. However, certain advertising cookies may constitute the "sale" or "sharing" of personal information for cross-context behavioural advertising under the CCPA/CPRA, the VCDPA, and similar state laws. To opt out, click the **Cookie Settings** link in our website footer and disable Marketing cookies in the preferences panel.

We do not knowingly sell or share the personal information of consumers under 16 years of age without affirmative authorisation (and, for consumers under 13, without parental consent).

13.4 Sensitive Personal Information

We do not use or disclose sensitive personal information (such as government identifiers, precise geolocation, account credentials, racial or ethnic origin, religious beliefs, or health information) for any purpose other than to provide the service you have requested, comply with our legal obligations, ensure security and integrity, or as otherwise permitted by applicable law. You have the right to limit our use of sensitive personal information by contacting us at the addresses above.

13.5 Profiling and Automated Decision-Making

We do not engage in profiling that produces legal or similarly significant effects concerning you without your consent. Where we use any automated processing (for example, AI-assisted candidate matching that you, as a controller, configure within the platform), meaningful human review remains available, and you may opt out of such processing by contacting us.

13.6 Global Privacy Control

We honour the Global Privacy Control (GPC) browser signal. If your browser transmits a GPC signal, we will treat it as a valid request to opt out of the sale and sharing of personal information for that browser and device, as required by the CCPA/CPRA, the CPA, and the CTDPA.

14. Brazil Privacy Rights (LGPD)

If you are located in Brazil, the Brazilian General Data Protection Law (Lei Geral de Proteção de Dados — Law No. 13,709/2018, or "LGPD") applies to our processing of your personal data. As a controller under the LGPD, we process your personal data based on one of the legal bases set out in Article 7 (or, for sensitive personal data, Article 11), including consent, performance of a contract, compliance with a legal or regulatory obligation, the regular exercise of rights in judicial, administrative, or arbitral proceedings, the protection of life or physical safety, the protection of health, our legitimate interests, or credit protection.

14.1 Your Rights Under the LGPD

As a data subject under the LGPD, you have the following rights, exercisable free of charge at any time (Article 18):

- **Confirmation and access:** Confirm the existence of processing and access your personal data
- **Correction:** Request the correction of incomplete, inaccurate, or out-of-date data
- **Anonymisation, blocking, or deletion:** Request anonymisation, blocking, or deletion of unnecessary or excessive data, or of data processed in non-compliance with the LGPD
- **Portability:** Request the portability of your data to another service or product provider, subject to commercial and industrial secrecy
- **Deletion of data processed with consent:** Request deletion of personal data processed on the basis of consent, except where retention is permitted by Article 16
- **Information about sharing:** Receive information about public and private entities with which we have shared your data
- **Information about consent:** Be informed about the possibility of not providing consent and the consequences of refusal
- **Revocation of consent:** Revoke your consent at any time through a simple and free procedure, with confirmation of receipt
- **Review of automated decisions:** Request review of decisions taken solely on the basis of automated processing that affects your interests

14.2 How to Exercise Your LGPD Rights

You can exercise your LGPD rights by:

- Emailing us at legal@wizardapplication.com (please indicate "LGPD Request" in the subject line).
- Submitting a privacy rights request via our contact form.

We will respond to your request within 15 days of receipt, as required by Article 19 of the LGPD. We may require reasonable verification of your identity before processing your request. You may also exercise your rights through a representative duly authorised in accordance with applicable

Brazilian regulations.

14.3 International Transfers from Brazil

Because our infrastructure is hosted in the United Kingdom and the European Economic Area, your personal data will be transferred outside Brazil. The LGPD permits such transfers where (a) the destination country provides an adequate level of protection, (b) the controller offers and demonstrates appropriate safeguards (such as standard contractual clauses, binding corporate rules, or specific contractual clauses), (c) the transfer is necessary for international cooperation, the protection of life, the performance of a contract to which the data subject is a party, the regular exercise of rights in judicial proceedings, compliance with a legal obligation, or the execution of a public policy, or (d) the data subject has given specific and informed consent for the transfer. We rely primarily on appropriate safeguards (standard contractual clauses with our sub-processors) and contractual necessity for transfers from Brazil.

14.4 Data Protection Officer for Brazil

We have designated an internal contact who serves as our point of communication for Brazilian data subjects and for the Autoridade Nacional de Proteção de Dados (ANPD):

- **Email:** legal@wizardapplication.com (please indicate "Encarregado — LGPD" in the subject line)

14.5 Right to Complain to the ANPD

If you believe that our processing of your personal data violates the LGPD, you have the right to lodge a complaint with the Autoridade Nacional de Proteção de Dados (ANPD), the Brazilian data protection authority:

- **Website:** www.gov.br/anpd

15. Japan Privacy Rights (APPI)

If you are located in Japan, the Act on the Protection of Personal Information (..... — the "APPI"), as enforced by the Personal Information Protection Commission (..... — the "PPC"), applies to our processing of your personal information. We comply with the APPI as a Personal Information Handling Business Operator (PIHBO) where its extraterritorial provisions apply, and we benefit from the reciprocal adequacy framework between the European Union, the United Kingdom, and Japan, which the PPC and the European Commission recognise as providing equivalent levels of protection.

15.1 Your Rights Under the APPI

As a data subject under the APPI, you have the following rights:

- **Disclosure (access):** Request disclosure of the personal information we hold about you, including in an electronic format where reasonably feasible
- **Correction, addition, or deletion:** Request correction, addition, or deletion of personal information that is inaccurate, incomplete, or out of date
- **Suspension of use or third-party provision:** Request that we cease using, delete, or stop providing your personal information to third parties where the legal grounds set out in Article 35 of the APPI are met
- **Disclosure of records of third-party provision:** Request disclosure of our records of provision of personal information to third parties
- **Opt-out of third-party provision:** Where we provide personal information to third parties by way of opt-out, you may object to such provision (we do not currently rely on the opt-out exemption under Article 27)

15.2 How to Exercise Your APPI Rights

You can exercise your APPI rights by:

- Emailing us at legal@wizardapplication.com (please indicate "APPI Request" in the subject line).
- Submitting a privacy rights request via our contact form.

We will respond to verifiable requests without undue delay, generally within two weeks of receipt, in accordance with PPC guidelines. We may require reasonable verification of your identity (and, where applicable, of any authorised representative acting on your behalf) before processing your request. There is no charge for the first request in a given period.

15.3 Special Care-Required Personal Information

"Special care-required personal information" (.....) under the APPI includes information on race, creed, social status, medical history, criminal record, status as a victim of crime, and certain physical or mental disabilities. We do not collect or process such information without your prior explicit consent, save where the acquisition is permitted without consent under Article 20(2) of the APPI (for example, where required by law, or where necessary for the protection of life, body, or property).

15.4 International Transfers from Japan

Our infrastructure is hosted in the United Kingdom and the European Economic Area. The PPC has recognised the EU and the UK as offering an equivalent level of personal information protection to Japan under the reciprocal adequacy frameworks adopted in 2019 (EU) and following the UK's post-Brexit continuity arrangements. Accordingly, transfers of personal information from Japan to our UK and EEA infrastructure are made in accordance with Article 28 of the APPI. In addition, we maintain appropriate safeguards including:

- Standard contractual clauses with our sub-processors where required
- Encryption in transit (TLS 1.3) and at rest (AES-256) in every region where personal information is stored or processed
- Compliance with the EU GDPR and UK GDPR, which the PPC recognises as providing protections substantially equivalent to or stronger than the APPI baseline

15.5 Mandatory Breach Notification

Under the APPI as amended in 2022, where a personal information breach affects individuals located in Japan and is likely to harm their rights and interests, we will notify the PPC promptly and notify affected individuals without undue delay, in accordance with the timelines, content, and method requirements set out in the APPI and PPC guidelines (including the obligation to provide a preliminary report within approximately three to five days, followed by a full report within thirty days, or sixty days in the case of unauthorised use for fraudulent purposes).

15.6 Right to Complain to the PPC

If you believe that our processing of your personal information violates the APPI, you have the right to lodge a complaint with the Personal Information Protection Commission (.....):

- **Website:** www.ppc.go.jp

16.3 Personal Data of Children

For Data Principals under the age of 18, we obtain verifiable consent from the parent or lawful guardian before processing personal data, and we do not undertake tracking, behavioural monitoring, or targeted advertising directed at children. Tenants who collect personal data of children through our platform are responsible for obtaining verifiable parental consent before submitting that data for processing.

16.4 Grievance Officer

In accordance with Section 8(10) of the DPDP Act, you may raise any concerns about our processing of your personal data with our Grievance Officer:

- **Name:** Data Protection Officer, Wizard Software Solutions Ltd
- **Email:** legal@wizardapplication.com
- **Response time:** We will acknowledge your grievance within seven (7) days and respond substantively within thirty (30) days

16.5 Cross-Border Transfers

Personal data of individuals located in India may be transferred outside India in accordance with the

DPDP Act, subject to any restrictions notified by the Central Government on transfers to specified jurisdictions. Where data residency is required, tenants may select an Indian AWS region (such as ap-south-1, Mumbai) during account setup.

16.6 Breach Notification

In the event of a personal data breach affecting Data Principals in India, we will notify the Data Protection Board of India and each affected Data Principal in accordance with the form, manner, and timelines prescribed under the DPDP Act and any rules notified under it.

16.7 Significant Data Fiduciary

If we are notified by the Central Government as a Significant Data Fiduciary under the DPDP Act, we will appoint a Data Protection Officer based in India, undertake periodic data protection impact assessments, and comply with the additional obligations notified to us.

17. Changes to This Privacy Policy

We may update our Privacy Policy from time to time to reflect changes in our practices, technology, legal requirements, or other factors. We will notify you of any material changes by:

- Posting the new Privacy Policy on this page
- Updating the "Last Updated" date at the top of this policy
- Sending an email notification to the address associated with your account for material changes
- Displaying a prominent notice within our service

For significant changes that require consent, we will obtain your explicit consent before the changes take effect. You are advised to review this Privacy Policy periodically to stay informed about how we protect your information.

Changes are effective when posted on this page. Your continued use of the service after changes are posted constitutes your acceptance of the revised Privacy Policy, unless the changes require explicit consent.

18. Contact Us

If you have any questions about this Privacy Policy, our data practices, or wish to exercise your privacy rights, please contact us:

18.1 General Privacy Enquiries

- **Email:** legal@wizardapplication.com
- **Response Time:** Within 48 hours for general enquiries

18.2 Data Protection Officer

- **Email:** legal@wizardapplication.com
- **Postal Address:**

Data Protection Officer
Wizard Software Solutions Ltd
30 Circus Mews
Bath, BA1 2PW
United Kingdom

18.3 Company Information

- **Company Name:** Wizard Software Solutions Ltd
- **Company Number:** 16878600

18.4 Supervisory Authority

If you are located in the UK, you have the right to lodge a complaint with the Information Commissioner's Office (ICO):

- **Website:** www.ico.org.uk
- **Phone:** 0303 123 1113
- **Address:** Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF

Last updated: 13 June 2026