# User, Visitor and Candidate Privacy Policy

**Effective date:01.06.2026**
**Version:** 1.0
**Website and application: www.inthecity.app**
**Controller / Operator:Benicia Francis Fernandez**
**Registered office: B01G39D, New Service Block - Al Hulaila FZ, B01G39D, Al Hulaila Industrial Free Zone RAK, United Arab Emirates**
**Licence number: 47022221**
**Privacy contact:+971508718966**
**General contact: +971508718966**
**Data Protection Officer / privacy lead: Benicia Francis Fernandez**

## 1. Purpose of this Privacy Policy

This Privacy Policy explains how **In The City FZ-LLC** collects, uses, shares, stores, protects, and otherwise processes personal data when individuals use the In The City website, mobile application, marketplace, advertising services, accommodation services, real estate advertising services, event advertising services, general advertising services, job advertisement services, payment features, account features, customer support channels, and related services.

This Policy is intended to comply with the transparency, fairness, accountability, data-subject rights, security, retention, transfer, and governance requirements of the EU General Data Protection Regulation where it applies, and the UAE federal personal data protection framework**,** including the UAE Personal Data Protection Law. Where any applicable data protection law gives you stronger rights than this Policy, the stronger mandatory legal standard will apply.

This Policy applies to **Customers**, registered users, unregistered visitors, persons who browse listings, persons who contact Suppliers through the Platform, persons who place orders, persons who make accommodation enquiries or bookings, persons who use payment features, persons who upload or publish CVs, job candidates, private advertisers, persons who communicate with customer support, and any other individuals whose personal data is processed in connection with the Platform.

## 2. Important definitions

For the purposes of this Policy, personal data means any information relating to an identified or identifiable natural person. This can include names, contact details, identifiers, account information, payment-related identifiers, order history, location information, device information, photographs, CVs, communications, and any other information that can identify or relate to a person.

**Processing** means any operation performed on personal data, including collection, recording, storage, organisation, use, disclosure, transfer, restriction, erasure, or destruction.

**Platform** means the i n t h e c i t y . a p p website, mobile application, marketplace, advertising, job, accommodation, real estate, event, payment, communication, account, and support features operated or made available by the Operator.

**Supplier** means a merchant, service provider, accommodation provider, advertiser, employer, real estate advertiser, event advertiser, private advertiser, or other person or entity offering goods, services, advertisements, accommodation, employment opportunities, or other content through or in connection with the Platform.

**Customer** means a person who uses the Platform to browse, contact Suppliers, place orders, make bookings, respond to advertisements, upload or publish CVs, or otherwise use Platform services.

## 3. Who is responsible for your personal data

For most Platform account, registration, browsing, payment orchestration, security, fraud prevention, ranking, marketing, support, and compliance activities**,** In The City FZ-LLC acts as the controller of your personal data because it determines why and how that data is processed.

Suppliers may act as separate controllers when they receive your personal data for their own purposes, such as fulfilling an order, providing accommodation, responding to your enquiry, contacting you about a job application, handling a complaint, issuing documentation, complying with their legal duties, or conducting their own customer service. Where Suppliers are separate controllers, they are responsible for their own privacy notices and their own compliance with applicable data protection laws.

In some circumstances, the Operator and a Supplier may jointly determine certain processing purposes or means, for example where specific Platform functionality is designed for both Platform operation and Supplier fulfilment. Where this occurs, the Operator will allocate responsibilities with the relevant Supplier and will provide the main points of the arrangement to affected users where required.

| Processing context | Primary responsibility | Practical explanation |
|---|---|---|
| Account creation, login, security, fraud prevention, Platform management | Operator | The Operator controls the Platform account and security environment. |
| Browsing, search, ranking, advertising display, and Platform analytics | Operator | The Operator controls how listings are displayed and how Platform performance is measured. |
| Order placement through the marketplace | Operator and Supplier, depending on activity | The Operator operates the Platform and payment point; the Supplier fulfils the contract. |
| Supplier fulfilment, delivery, accommodation, complaints, and after-sales communications | Supplier | The Supplier uses your order or enquiry data to perform its contract with you. |
| Payment processing | Operator and payment providers, with possible Supplier settlement data | Payment providers process payment data under their own terms and privacy notices. |
| CV upload, CV sending, CV publication, and employer contact | Operator and relevant Suppliers | The Operator provides the CV functionality; Suppliers use CVs for recruitment purposes. |
| Legal compliance, claims, fraud investigation, regulator response | Operator, Supplier, or both depending on the matter | Each party may need to keep and use data to comply with legal obligations or defend rights. |

## 4. Personal data we collect

We collect personal data directly from you, automatically through your use of the Platform, from Suppliers, from payment providers, from service providers, and from public or legally available sources where necessary for verification, fraud prevention, compliance, or dispute handling.

| Category of data | Examples | Source |
|---|---|---|
| Identity data | Name, surname, username, account identifier, age confirmation, customer number | You, Platform account records |
| Contact data | Email address, telephone number, delivery or booking contact details | You, Supplier communications, support records |
| Account data | Login credentials, account settings, preferences, account status, registration date, consent records | You, Platform systems |
| Order and transaction data | Goods or services ordered, order status, delivery details, booking details, cancellation, complaint, refund, chargeback, payment status | You, Suppliers, payment providers |
| Payment-related data | Payment method type, transaction ID, amount, currency, confirmation, refund status, fraud flags, settlement reference | You, Stripe, card networks, wallet providers, Suppliers |
| Communication data | Messages to Suppliers, support tickets, emails, SMS, in-app messages, notices, call notes where applicable | You, Suppliers, support channels |
| Advertising and listing interaction data | Searches, clicks, viewed listings, contact requests, boosted listing interactions, enquiry data | You, Platform systems |

| Category of data | Examples | Source |
|---|---|---|
| Accommodation and booking data | Accommodation dates, number of guests, special requests, booking status, cancellation details | You, Suppliers |
| Real estate enquiry data | Property listing interactions, contact requests, messages to advertisers or brokers | You, Suppliers or advertisers |
| Event interaction data | Event listings viewed, enquiries, bookings or expressions of interest where applicable | You, Suppliers or event advertisers |
| CV and recruitment data | CV, employment history, education, skills, photograph if uploaded, salary expectations if included, application messages, publication settings | You, Suppliers/employers |
| Technical and device data | IP address, device type, operating system, browser type, app version, language, time zone, cookie identifiers, log data | Your device, Platform systems |
| Approximate or precise location data | City, country, approximate location from IP address, precise location if you enable location permissions | Your device, Platform systems |
| Fraud, trust, and safety data | Risk signals, device identifiers, suspicious activity records, account misuse flags, identity or payment verification status | Platform systems, payment providers, Suppliers |
| Marketing preference data | Newsletter consent, direct marketing opt-in or opt-out, communication preferences | You, Platform systems |
| Legal and compliance data | Records needed for legal claims, regulatory requests, complaints, accounting, tax, audit, law enforcement, or statutory retention | You, Suppliers, authorities, Platform systems |

## 5. Special category and sensitive personal data

The Platform is not designed to collect sensitive personal data unless this is necessary for a specific feature or you choose to include it in content you upload. Sensitive or special-category data may include health information, biometric information, racial or ethnic origin, political opinions, religious beliefs, trade union membership, genetic data, sexual orientation, family background, criminal record, or similar protected categories under applicable law. Under UAE Federal Decree-Law No. 45 of 2021, sensitive data also expressly includes family background and criminal record as distinct protected categories.

You should not include unnecessary sensitive information in messages, advertisements, reviews, support requests, or CVs. If you upload a CV, you should include only information that is relevant to employment opportunities. If you choose to include sensitive information in a CV or message, the Operator and relevant Suppliers may process that information to provide the requested recruitment or communication functionality, subject to applicable law.

Where we intentionally need to process sensitive personal data, we will do so only where a valid legal basis and any additional condition required by applicable law exists, such as explicit consent, legal obligation, establishment or defence of legal claims, protection of vital interests, or another permitted basis.

## 6. Why we process personal data and our lawful bases

We process personal data only where we have a lawful basis. Under GDPR, the lawful bases may include performance of a contract, steps before entering a contract, legal obligation, legitimate interests, consent, vital interests, or public interest where applicable. Under UAE data protection requirements, processing must be fair, transparent, legitimate, limited to clear purposes, secure, and supported by an appropriate lawful basis such as consent, contract, legal obligation, protection of interests, public interest, or another permitted basis.

| Purpose | Data used | GDPR lawful basis where GDPR applies | UAE basis or compliance rationale |
|---|---|---|---|
| Registering and managing your account | Identity, contact, account, credential, age confirmation, device and security data | Contract; legitimate interests in account security; legal obligation where applicable | Contract performance; legitimate and transparent account management; security and compliance |
| Allowing you to browse and use Platform features | Technical, device, listing interaction, search, preference, location where enabled | Contract; legitimate interests; consent for non-essential cookies where required | Provision of requested services; consent where required; transparency and purpose limitation |
| Facilitating marketplace orders | Identity, contact, order, delivery, payment status, messages | Contract; legitimate interests in operating the marketplace; legal obligation | Contract implementation; Platform operation; compliance and dispute handling |
| Sharing order details with Suppliers | Identity, contact, order, delivery, booking, enquiry and complaint data | Contract; legitimate interests; legal obligation where applicable | Necessary to complete requested Supplier transaction or enquiry |
| Processing payments and refunds | Payment-related data, transaction data, fraud data, account data | Contract; legal obligation; legitimate interests in fraud prevention | Contract implementation; legal compliance; security and fraud prevention |
| Providing accommodation, real estate, event, and advertising contact features | Identity, contact, enquiry, booking, listing interaction and message data | Contract; legitimate interests | Provision of requested Platform and Supplier communication services |

| Purpose | Data used | GDPR lawful basis where GDPR applies | UAE basis or compliance rationale |
|---|---|---|---|
| Allowing CV upload, CV sending, and CV publication | CV, identity, contact, recruitment messages, publication settings, access logs | Consent for publication; contract or request before contract for application; legitimate interests in platform security | Consent and requested recruitment functionality; data-subject control; security |
| Operating ranking, search, boosted listings, and recommendations | Search, location, listing interaction, account preferences, listing metadata | Legitimate interests; consent where profiling or cookies require it | Transparent Platform operation and advertising display; consent where required |
| Sending service communications | Contact, account, order and support data | Contract; legitimate interests | Service administration and transactional notifications |
| Sending marketing communications | Contact, preferences, consent records, interaction data | Consent where required; legitimate interests where permitted with opt-out | Consent-led marketing and opt-out control |
| Preventing fraud, misuse, unauthorised access, and policy violations | Account, technical, device, payment, fraud, log and communication data | Legitimate interests; legal obligation; contract | Security, fraud prevention, legal compliance, protection of users and Suppliers |
| Customer support and complaint handling | Identity, contact, messages, order, payment, technical and complaint data | Contract; legitimate interests; legal obligation | Support, dispute resolution, compliance, and claims management |
| Complying with law and responding to authorities | Identity, contact, transaction, logs, communications, legal records | Legal obligation; legitimate interests | Compliance with UAE and other applicable laws, regulator or court requests |

| Purpose | Data used | GDPR lawful basis where GDPR applies | UAE basis or compliance rationale |
|---|---|---|---|
| Establishing, exercising or defending legal claims | Relevant account, order, payment, communication, technical and legal data | Legitimate interests; legal obligation | Protection and defence of rights and legal claims |
| Improving the Platform | Technical, usage, support, aggregated or anonymised analytics data | Legitimate interests; consent for non-essential cookies where required | Service improvement with transparency, minimisation and security |

Where we rely on consent, you may withdraw consent at any time through the relevant Platform settings or by contacting us. Withdrawal of consent does not affect processing that took place lawfully before withdrawal. Where processing is required for a contract or legal obligation, withdrawal of consent may not stop processing that is necessary for that contract or obligation.

## 7. Marketplace orders and Supplier data sharing

When you place an order, request a booking, contact a Supplier, respond to a listing, or submit information through a Supplier-facing feature, we share the information necessary for that transaction or communication with the relevant Supplier. This may include your name, contact details, order or enquiry details, delivery or booking information, payment status, messages, complaint details, and other information needed to fulfil the transaction.

Suppliers must use Platform-originating Customer data only for authorised purposes, including fulfilment, customer support, delivery, accommodation, recruitment where applicable, legal compliance, fraud prevention, dispute handling, and communications requested by you. Suppliers must not use Customer data received through the Platform for unrelated marketing, resale, profiling, enrichment, or disclosure unless they have a separate lawful basis and have given you any legally required notice.

You should review the Supplier's own terms and privacy notice before completing a transaction where they are made available. If a Supplier fails to provide an adequate privacy notice or misuses your data, you may contact us at support@inthecity.app and we may take appropriate Platform action under our Supplier terms.

## 8. Payments, Stripe, cards, and wallet providers

Payments on the Platform may be processed through third-party payment providers, including Stripe, card networks, banks, Google Pay, Apple Pay, and other supported payment methods. These providers may process your payment information under their own terms and privacy notices. We may receive and store payment-related information such as transaction ID, payment status, amount, currency, refund status, chargeback status, risk indicators, payment method type, and limited card information such as last four digits where made available. Unless expressly stated otherwise, we do not store full payment card numbers.

We use payment-related data to process orders, confirm payment, issue receipts or confirmations, transfer funds to Suppliers where applicable, handle refunds and chargebacks, prevent fraud, reconcile accounts, comply with accounting and tax duties, and respond to disputes or legal requests.

| Payment data context | Who may receive data | Purpose |
|---|---|---|
| Card or wallet payment | Payment provider, card network, wallet provider, bank | Payment authorisation, fraud checks, settlement, refund, chargeback |
| Marketplace settlement | Operator, Supplier, payment provider | Confirmation that payment was made and settlement can occur |
| Refund or chargeback | Operator, Supplier, payment provider, bank/card network | Refund processing, dispute evidence, account reconciliation |
| Fraud or misuse investigation | Operator, payment provider, Supplier where relevant, authorities where legally required | Security, fraud prevention, legal compliance |

## 9. CVs, job applications, and candidate visibility

The Platform may allow you to upload a CV, send a CV to a particular Supplier or employer, and, if you choose, publish your CV for viewing by Suppliers or employers through the Platform. These are separate actions. Sending a CV to a specific Supplier does not automatically mean that your CV is published generally. Publishing a CV makes it available according to the visibility settings shown to you at the time of publication.

Before you upload or publish a CV, you should ensure that the content is accurate, relevant, and limited to information needed for employment or professional contact. You should avoid including unnecessary sensitive information. If the Platform allows you to add a photo, nationality, date of birth, salary expectations, visa status, health information, or other sensitive or high-risk information, you should include such information only where it is necessary and lawful for the relevant opportunity.

| CV action | What happens | Control available to you |
|---|---|---|
| Upload CV privately | The CV is stored in your account or candidate profile if this feature is available | You may edit or delete it, subject to legal retention exceptions. |
| Send CV to a Supplier | The selected Supplier receives your CV and related message | You may request information about recipients and may exercise applicable rights. |
| Publish CV for Suppliers | Suppliers with relevant access may view your CV according to Platform settings | You may unpublish it, change visibility settings, or delete it where available. |
| Supplier contacts you | A Supplier may use the Platform or contact details you provided for recruitment | You may object to further contact where legally available. |

Suppliers receiving CVs must use them only for recruitment or professional contact purposes connected with the relevant job opportunity or candidate visibility feature. They must not use CVs for unrelated marketing, disclose them to unauthorised parties,

retain them longer than necessary, or use them unlawfully. If you believe a Supplier has misused your CV, contact us at support@inthecity.app

## 10. Advertising, ranking, boosted listings, recommendations, and automated systems

The Platform may display listings, advertisements, goods, services, accommodation, real estate, events, job advertisements, and other content according to ranking parameters such as category, city, location, relevance, availability, user search terms, listing quality, recency, Supplier status, paid boosting, user preferences, and Platform rules. Some listings may be marked or treated as promoted, sponsored, boosted, or otherwise prioritised.

We may use automated systems for account registration, order creation, payment status, fraud prevention, abuse detection, ranking, search results, listing display, security alerts, and service notifications. These systems help operate the Platform efficiently and securely. If we use automated processing that produces legal or similarly significant effects on you, you may request human review or challenge the decision where applicable law gives you that right.

Automated decisions that may restrict your account, reject a payment, or limit your access to the Platform are significant automated decisions under applicable data protection law. If you believe such a decision has been made about you, you may contact us at support@inthecity.app to request human review of that decision. We will acknowledge your request and respond within the timeframe required by applicable law.

| Automated or ranking activity | Data potentially used | Impact on you | Your control |
|---|---|---|---|
| Search and listing ranking | Search terms, city, category, listing metadata, paid boosting, preferences | Determines the order or prominence of results | You can adjust searches, filters, location settings, and preferences where available. |

| Automated or ranking activity | Data potentially used | Impact on you | Your control |
|---|---|---|---|
| Fraud and abuse checks | Account, device, payment, log, order, communication and risk data | May delay, block, restrict, or review activity | You may contact support to request review where appropriate. |
| Payment processing | Payment status, provider response, transaction risk data | Payment may be authorised, rejected, delayed, refunded, or reviewed | You may contact the payment provider or Platform support. |
| CV visibility | Publication settings, account status, candidate profile data | Determines whether Suppliers can view your CV | You may change visibility or unpublish where available. |

## 11. Cookies, analytics, and similar technologies

We may use cookies, SDKs, pixels, local storage, device identifiers, and similar technologies to operate the Platform, remember preferences, secure accounts, detect fraud, measure performance, improve services, and, where permitted, provide analytics or marketing. Some technologies are strictly necessary for the Platform to function. Others, such as analytics or marketing cookies, may require consent depending on your location and applicable law.

Where required, we will present a cookie banner or preference centre allowing you to accept, reject, or manage non-essential cookies. You may also manage cookies through your browser or device settings. If you disable certain cookies, some Platform features may not work properly.

## 12. Direct marketing and service communications

We may send you service communications related to your account, orders, bookings, payments, security, legal notices, policy updates, and support. These are not marketing messages and may be necessary to provide the Platform.

We will send direct marketing only where we have a valid basis to do so. Where consent is required, we will ask for consent before sending marketing. You may opt

out of marketing at any time by using the unsubscribe link, changing your account preferences, or contacting us. Opting out of marketing does not stop necessary service communications.

## 13. Who we share personal data with

We share personal data only where necessary for the purposes described in this Policy, where you have directed us to share it, where required by law, or where otherwise permitted by applicable data protection law.

| Recipient category | Examples | Purpose |
|---|---|---|
| Suppliers | Merchants, service providers, accommodation providers, advertisers, employers, real estate advertisers, event organisers | Order fulfilment, bookings, enquiries, recruitment, complaints, customer communication |
| Payment providers | Stripe, card networks, banks, Apple Pay, Google Pay, wallet providers | Payment processing, settlement, fraud prevention, refunds, chargebacks |
| Hosting and IT providers | Cloud hosting, storage, security, infrastructure, app services | Platform operation, storage, backup, security, maintenance |
| Communication providers | Email, SMS, push notification, customer-support platforms | Service notices, account messages, support, marketing where permitted |
| Analytics and performance providers | Analytics, crash reporting, diagnostic services | Platform performance, troubleshooting, service improvement |
| Professional advisers | Lawyers, auditors, accountants, consultants, insurers | Legal advice, audit, accounting, compliance, claims |
| Authorities and courts | Regulators, law enforcement, courts, government bodies | Legal compliance, lawful requests, claims, investigations |

| Recipient category | Examples | Purpose |
|---|---|---|
| Corporate transaction parties | Potential buyer, investor, merger counterparty, advisers | Due diligence, restructuring, merger, acquisition, financing, sale of business |

We require service providers processing personal data for us to protect the data, use it only for authorised purposes, and comply with applicable contractual and legal obligations.

## 14. International transfers

The Operator is established in the United Arab Emirates. Your personal data may be processed in the UAE and in other countries where we, Suppliers, payment providers, hosting providers, support providers, communications providers, or other service providers operate. These countries may have data protection laws that differ from those in your country.

Where GDPR applies and personal data is transferred from the European Economic Area to a country that does not have an adequacy decision, we will use appropriate safeguards where required, such as standard contractual clauses, transfer risk assessments, supplementary measures, binding contractual protections, or another lawful transfer mechanism. Where UAE transfer rules apply, we will transfer personal data outside the UAE only where permitted by applicable law, such as where the destination provides appropriate personal data protection, where contractual or other safeguards are in place, where you have consented where required, where the transfer is necessary for a contract, legal obligation, protection of interests, public interest, or another permitted basis.

## 15. How long we keep personal data

We keep personal data only for as long as necessary for the purposes described in this Policy, unless a longer period is required or permitted by law. Retention periods

may vary depending on account status, transaction history, legal duties, dispute risk, fraud prevention needs, accounting obligations, and user choices.

| Data category | Typical retention period | Notes |
|---|---|---|
| Account data | Account lifetime plus [5 years after closure | Some data may be retained longer for disputes, fraud prevention, or legal compliance. |
| Order and booking data | [5] years from transaction completion | Needed for fulfilment, complaints, tax, accounting, refunds, chargebacks, and legal claims. |
| Payment and invoice records | [5] years or legally required accounting/tax period | Full card numbers should not be stored by the Operator unless expressly disclosed. |
| Support and complaint records | [5] years after closure of the issue | May be retained for quality, disputes, and legal claims. |
| CVs stored privately | Until deleted by you or account closure, subject to [5] | The Platform should provide deletion controls where technically available. |
| Published CVs | Until unpublished by you, expiry of publication period, or account closure | Recommended maximum publication period: [12] months unless renewed. |
| CVs sent to Suppliers | Operator record retained for [5] years; Supplier retention governed by Supplier obligations | Suppliers should delete when recruitment purpose ends unless legally required. |
| Marketing consent records | Until consent is withdrawn plus [5] years for proof | Used to evidence consent and opt-out compliance. |
| Security and fraud logs | [12] months/years depending on risk | Longer retention may apply to confirmed fraud, abuse, or legal disputes. |
| Cookie and analytics data | As stated in Cookie Notice | Non-essential cookies should follow consent settings where required. |

| Data category | Typical retention period | Notes |
|---|---|---|
| Legal claim records | Duration of claim plus applicable limitation period | May include relevant account, transaction, communication, and evidence records. |

When personal data is no longer needed, we will delete it, anonymise it, or securely restrict it unless continued retention is required by law or necessary for legal claims, fraud prevention, security, accounting, audit, or regulatory purposes.

## 16. How we protect personal data

We implement appropriate technical and organisational measures designed to protect personal data against unauthorised access, disclosure, alteration, loss, misuse, or destruction. These measures may include access controls, password and credential protection, encryption or pseudonymisation where appropriate, secure transmission, logging, backup, resilience measures, staff confidentiality, supplier and service provider controls, incident response, testing, and review.

No online service can guarantee absolute security. You are responsible for keeping your login details confidential, using strong passwords, securing your devices, and notifying us immediately if you suspect unauthorised access to your account.

## 17. Personal data breaches

If we become aware of a personal data breach affecting your data, we will investigate, take appropriate mitigation steps, and notify regulators or affected individuals where required by applicable law. Where required to notify a regulatory authority, we will aim to do so within 72 hours of becoming aware of the breach, or as soon as reasonably practicable, in line with international best practice and any timelines prescribed by the UAE Data Office or other competent authority. Where a breach is likely to result in a high risk to your rights, we will notify you directly without undue delay If a Supplier or service provider becomes aware of a breach affecting Platform personal data, we require them to notify us and cooperate with investigation and mitigation.

If you believe your account or personal data has been compromised, contact us immediately at support@inthecity.app

## 18. Your data protection rights

Depending on the law that applies to your personal data, you may have rights to request access, correction, deletion, restriction, portability or transfer, objection to processing, withdrawal of consent, information about processing, objection to direct marketing, objection to or challenge certain automated decisions, and complaint to a supervisory authority.

| Right | What it means |
|---|---|
| Access | You may request confirmation of whether we process your personal data and receive a copy of it. |
| Correction | You may request correction or completion of inaccurate or incomplete data. |
| Deletion | You may request deletion where the data is no longer needed, consent is withdrawn, processing is unlawful, or another legal ground applies. |
| Restriction | You may request temporary restriction of processing in certain circumstances. |
| Portability or transfer | You may request data you provided in a structured, commonly used, machine-readable format or request transfer where technically feasible and legally required. |
| Objection | You may object to certain processing based on legitimate interests, public interest, scientific/statistical processing, or direct marketing. |
| Withdraw consent | You may withdraw consent where processing is based on consent. |
| Automated decision challenge | You may request review or challenge certain decisions made solely by automated processing where legally available. |
| Complaint | You may complain to the relevant data protection authority or regulator. |

To exercise your rights, contact us at support@inthecity.app or use the rights request form at www.inthecity.app may need to verify your identity before responding. We will respond within the time required by applicable law. Where GDPR applies, we will generally respond within one month, subject to lawful extensions for complex requests. We will not charge a fee unless a request is manifestly unfounded, excessive, repetitive, or otherwise chargeable under applicable law.

## 19. Complaints and supervisory authorities

You may contact us first so we can try to resolve your concern promptly. If you are located in the UAE, you may have the right to complain to the competent UAE data protection authority or other competent authority when available. The national data protection regulator in the UAE is the UAE Data Office, established under Federal Decree-Law No. 44 of 2021. We will update this section with the UAE Data Office's complaint contact details when it is fully operational and accepting complaints from the public. If you are located in the European Economic Area, you may have the right to complain to your local data protection supervisory authority.

Our privacy contact is: **Benicia Francis Fernandez**
Our postal address is:
**B01G39D, New Service Block - Al**
**Hulaila FZ, B01G39D, Al Hulaila Industrial Free Zone**
**RAK, United Arab Emirates**

## 20. Children and age restrictions

The Platform is intended for users who are at least 18 years old unless a specific service expressly states otherwise. We do not knowingly allow persons under 18 to register as Customers. If we learn that a person under 18 has created an account or provided personal data contrary to our terms, we may delete or restrict the account and related data unless retention is legally required.

## 21. Third-party websites and Supplier platforms

The Platform may contain links to Supplier websites, payment providers, app stores, social media pages, external advertisements, and third-party services. This Policy does not apply to third-party websites or services that are not controlled by the

Operator. You should review the privacy notice of any third party before providing personal data to them.

## 22. Changes to this Policy

We may update this Policy from time to time to reflect changes in the Platform, legal requirements, processing activities, service providers, or operational practices. The updated version will be published at www.inthecity.app.If changes are material, we will provide reasonable notice through the Platform, email, app notification, or another appropriate method where required.

The effective date and version number at the top of this Policy show when it was last updated. Previous versions may be archived for legal and accountability purposes.

## 23. Contact details

For privacy questions, rights requests, complaints, or concerns, contact:

| Contact | Details |
|---|---|
| Controller | **Benicia Francis Fernandez** |
| Registered office | **B01G39D, New Service Block - Al Hulaila FZ, B01G39D, Al Hulaila Industrial Free Zone, RAK, United Arab Emirates** |
| Privacy email | support@inthecity.app |
| General email | inthecityl@inthecity.app |
| DPO / privacy lead | NO |
| Rights request form | www.inthecity.app |

## 24. Internal legal reference note

This Policy has been drafted to address transparency, controller/processor role clarity, data-subject rights, lawful basis, security, breach, transfer, retention, and automated-

processing requirements reflected in GDPR relevant articles, and in UAE PDPL compliance summaries concerning fair and transparent processing, controller and processor obligations, records, security, breach notification, rights, DPIA-style assessments, and cross-border transfers.