



PRIVACY POLICY

Personal Data Protection Notice

Last Updated: [20/07/2026]

Version: [1.0]

[Bayata Company for Information Technology]

Commercial Registration No. [7033191102]

[Damman Rd., Al Yarmuk Dist. Riyadh, Postal Code: 13251]

Kingdom of Saudi Arabia

Table of Contents

Table of Contents.....	2
Privacy at a Glance.....	4
1. Who We Are and Scope of this Policy.....	5
1.7 Independent controllers.....	5
2. Definitions	5
3. Principles We Apply	6
4. Personal Data We Collect	6
4.1 Data you provide directly	6
4.2 Data collected automatically	7
4.3 Data from third parties.....	7
4.4 Sensitive Data	7
5. Purposes and Legal Bases.....	8
6. Device Permissions	9
7. Disclosure and Sharing of Personal Data.....	9
7.3 To other users	9
7.4 To service providers acting as Data Processors	10
7.5 To authorities and for legal reasons	10
7.6 Corporate transactions.....	10
8. Cookies, SDKs and Similar Technologies.....	10
8.4 Apple App Tracking Transparency	11
8.5 Managing your choices.....	11
9. International Transfers of Personal Data	11
10. Retention of Personal Data	12
11. Your Rights	12
11.2 Right to be informed	13
11.3 Right of access and to obtain a copy	13
11.4 Right to correction and to deletion	13
11.5 Right to portability	13
11.6 Right to object and to restrict processing	13
11.7 Right to withdraw consent.....	13
11.8 Rights relating to automated decisions.....	13
11.9 How to exercise your rights	13
11.10 Right to complain.....	14
12. Automated Processing and Artificial Intelligence.....	14
13. Children’s Privacy.....	14
14. Security of Personal Data	14
14.3 Incident response and breach notification	15
15. App Store Privacy Disclosures	15
15.2 Apple App Store — privacy label summary.....	15

15.3 Google Play — Data Safety summary	15
15.4 Account and data deletion route	16
16. Changes to this Policy	16
17. Contact Us	16

Privacy at a Glance

This summary is provided for convenience only. It does not replace the full Policy set out below, and it does not form part of it.

Question	Short answer
Who is responsible for your data?	The Company, as Data Controller. See Clause 1.
What do we collect?	Account and identity data, booking and payment data, communications, device and usage data, location, and media you upload. See Clause 4.
Why do we collect it?	To operate the marketplace, verify users, process payments, keep the platform safe, comply with law, and improve the service. See Clause 5.
Do we sell your data?	No. We do not sell personal data and we do not share it with advertisers for cross-app tracking.
Who do we share it with?	Other users to the extent needed for a booking, service providers, payment providers, and authorities where legally required. See Clause 7.
Do we transfer data abroad?	Only where permitted under the PDPL and its Implementing Regulations, with safeguards. See Clause 9.
What rights do you have?	Access, correction, deletion, portability, objection, withdrawal of consent, and complaint to SDAIA. See Clause 11.
How long do we keep it?	For as long as your account is active, then for defined retention periods. See Clause 10.
Children?	The Platform is for adults aged 18+. We do not knowingly collect children's data. See Clause 13.

1. Who We Are and Scope of this Policy

- 1.1 This Privacy Policy explains how [Bayata Company for Information Technology], a company incorporated under the laws of the Kingdom of Saudi Arabia under Commercial Registration No. [7033191102], having its registered office at [Dammam Rd., Al Yarmuk Dist. Riyadh, Postal Code: 13251], (the "Company", "Talinoo", "we", "us" or "our") collects, uses, discloses, transfers, retains, and protects Personal Data in connection with the Talinoo mobile application and any associated website or service (together, the "Platform").
- 1.2 For the purposes of the Personal Data Protection Law promulgated by Royal Decree No. M/19 dated 09/02/1443H, as amended, and its Implementing Regulations (together, the "PDPL"), the Company is the Data Controller in respect of the Personal Data described in this Policy.
- 1.3 This Policy applies to all Users of the Platform, whether registered as Customers, as Talents, or both, and to visitors who interact with the Platform without registering.
- 1.4 This Policy forms part of, and should be read together with, the Talinoo Terms and Conditions. Capitalised terms not defined in this Policy have the meaning given to them in the Terms and Conditions. In particular, Clause 24 (Confidentiality and Data Protection) and Clause 29.3 (Artificial Intelligence and Automated Processing) of the Terms and Conditions are relevant to this Policy.
- 1.5 This Policy does not apply to: (a) the processing of your Personal Data by a Talent or a Customer acting as an independent controller in connection with a Service; or (b) any third-party website, application, or service which you access through a link on the Platform. Those parties have their own privacy policies, and you should review them.
- 1.6 This Policy is published in Arabic and English. In the event of any discrepancy or dispute as to interpretation, the Arabic version prevails.

1.7 Independent controllers

- 1.7.1 Where a Talent receives Personal Data about a Customer in order to perform a Booking (for example, the Customer's name, address, contact number, allergen information, or event details), that Talent processes the data as an independent Data Controller in its own right, and is separately responsible for its own compliance with the PDPL.
- 1.7.2 The Company requires Talents, under Clause 24.2.2 of the Terms and Conditions, to use such data only for the purpose of the Booking, to keep it secure, to retain it no longer than necessary, and not to use it for marketing without a lawful basis. The Company is not, however, responsible for a Talent's independent processing.

2. Definitions

2.1 In this Policy:

- "Data Controller" means the entity that determines the purpose and manner of processing Personal Data.
- "Data Processor" means an entity that processes Personal Data on behalf of, and under the instructions of, a Data Controller.
- "Personal Data" means any data, of whatever source or form, that identifies an individual or makes them identifiable, directly or indirectly.
- "Sensitive Data" means Personal Data revealing racial or ethnic origin, religious, intellectual or political belief, security or criminal data, biometric or genetic data identifying an individual, health data, and data indicating that an individual's parentage is unknown.

- "Processing" means any operation performed on Personal Data, including collection, recording, storage, organisation, use, disclosure, transfer, publication, blocking, erasure, and destruction.
- "SDAIA" means the Saudi Data and Artificial Intelligence Authority, the competent supervisory authority for personal data protection in the Kingdom of Saudi Arabia.
- "You" means the individual whose Personal Data is processed, being the Data Subject.

3. Principles We Apply

3.1 We process Personal Data in accordance with the following principles, which reflect the requirements of the PDPL:

- Lawfulness, fairness and transparency: we process data on a lawful basis and tell you what we do with it.
- Purpose limitation: we collect data for specific, declared, legitimate purposes and do not process it in a manner incompatible with those purposes.
- Data minimisation: we collect only what is necessary and proportionate for the declared purpose.
- Accuracy: we take reasonable steps to keep data accurate, complete and current, and to correct it where it is not.
- Storage limitation: we retain data only for as long as necessary for the declared purpose or as required by law, and then delete or anonymise it.
- Integrity and confidentiality: we apply appropriate technical, organisational and administrative safeguards.
- Accountability: we maintain records of processing activities and can demonstrate our compliance.

4. Personal Data We Collect

We collect Personal Data in three ways: data you provide to us directly; data generated automatically when you use the Platform; and data we receive from third parties.

4.1 Data you provide directly

Category	Examples
Account data	Full name, mobile number, email address, password (stored in hashed form), profile photograph, preferred language, city.
Identity and verification data	Saudi National ID or Iqama number, passport details, date of birth, gender, a photograph or scan of an identity document, and a selfie or liveness check used to confirm the document belongs to you. For Talents: commercial registration, freelance certificate, professional licence, health certificate, municipal permit, and insurance documents.
Talent profile data	Service categories, skills, portfolio images and videos, pricing, availability, service area, qualifications, and description of services offered.
Booking data	Service requested, date and time, service address or location, number of attendees, special requirements, allergen or dietary information you choose to provide, and event details.
Payment data	Billing name, transaction amount and history, and a masked card reference (last four digits and card type). For Talents: bank account name, IBAN, and payout history. Full card numbers are collected and stored by our licensed Payment Providers, not by us.

Category	Examples
Communications	Messages exchanged with other users through in-app messaging, and correspondence with our support team, including attachments.
User-generated content	Ratings, reviews, replies to reviews, photographs and videos you upload, reports and complaints you submit.
Tax data	VAT registration number and tax identification details, where you are a Talent required to provide them.

4.2 Data collected automatically

Category	Examples
Device data	Device model, operating system and version, unique device identifiers, mobile network, language and timezone settings, application version, and screen resolution.
Identifiers	Advertising identifier (IDFA on iOS, AAID on Android) where you consent to it; installation identifier; and internal user identifier.
Usage data	Pages and screens viewed, features used, search queries, listings viewed, buttons tapped, session duration, timestamps, and referral source.
Log and technical data	IP address, access times, crash logs, diagnostic data, error reports, and performance metrics.
Location data	Precise location (GPS) where you grant permission, and approximate location derived from your IP address. See Clause 6.
Cookies and similar technologies	Cookies, SDKs, pixels, and local storage used on our website and within the application. See Clause 8.

4.3 Data from third parties

- Payment Providers: transaction confirmations, authorisation results, chargeback notifications, and fraud signals.
- Identity verification providers: the result of document authenticity and liveness checks.
- Other users: information contained in a review, report, complaint, or dispute submission concerning you.
- Analytics and crash-reporting providers: aggregated and event-level usage data as described in Clause 8.
- Public and governmental sources: where required to verify a licence, a commercial registration, or a sanctions or watchlist screening result.

4.4 Sensitive Data

4.4.1 We do not seek to collect Sensitive Data except where it is strictly necessary and we have a lawful basis to do so. In limited circumstances Sensitive Data may arise, in particular:

- Health-related information you voluntarily disclose in a Booking (for example, an allergy, a dietary restriction, a pregnancy, or a mobility limitation you disclose so that the Service can be delivered safely);
- Biometric data used solely for identity verification, in the form of a facial-comparison or liveness check;
- Criminal or security data arising from background screening or from sanctions and watchlist checks.

4.4.2 Where we process Sensitive Data we rely on your explicit consent, on the protection of vital interests, or on a legal obligation, as applicable. You are not obliged to disclose health information to a Talent; if you choose not to, the Talent may be unable to deliver the Service safely.

5. Purposes and Legal Bases

5.1 We process your Personal Data for the purposes set out below. The table identifies the legal basis on which we rely under the PDPL. Where we rely on legitimate interests, we have assessed that our interest is not overridden by your rights and freedoms.

Purpose	Data used	Legal basis
Creating and administering your account	Account data, identity data	Performance of a contract
Verifying identity, licences and eligibility	Identity and verification data, biometric check result	Legal obligation; explicit consent (biometrics); legitimate interests (platform safety)
Displaying listings and enabling discovery and search	Talent profile data, location, usage data	Performance of a contract
Processing bookings and enabling communication between users	Booking data, communications, account data	Performance of a contract
Processing payments, payouts, refunds and chargebacks	Payment data, booking data	Performance of a contract; legal obligation
Calculating and collecting commission, and issuing tax invoices	Payment data, tax data	Performance of a contract; legal obligation
Fraud prevention, anti-money-laundering and sanctions screening	Identity data, payment data, device and log data	Legal obligation; legitimate interests
Trust and safety, investigating reports, moderating content, detecting circumvention	Communications, booking data, usage data, reports	Legitimate interests; legal obligation
Providing customer support and handling complaints and disputes	All relevant categories	Performance of a contract; legitimate interests
Service-related notifications (booking, payment, security, policy changes)	Account data, booking data	Performance of a contract
Marketing communications and promotions	Account data, usage data	Consent (withdrawable at any time)
Analytics, crash reporting and improving the Platform	Device, usage, log data	Consent (where required); legitimate interests
Personalisation, ranking and recommendations	Usage data, booking history, ratings	Legitimate interests; consent where required
Complying with legal, regulatory and judicial obligations	All relevant categories	Legal obligation
Establishing, exercising or defending legal claims	All relevant categories	Legitimate interests; legal obligation

- 5.2** Where we rely on your consent, you may withdraw it at any time in accordance with Clause 11.7. Withdrawal does not affect the lawfulness of processing carried out before withdrawal, and does not affect processing carried out on another lawful basis.
- 5.3** If we intend to process your Personal Data for a purpose materially different from those declared in this Policy, we will notify you and, where required, obtain your consent before doing so.

6. Device Permissions

- 6.1** The Platform requests the following device permissions. Each is optional, each is requested at the point of first use with an explanation of why it is needed, and each may be refused or revoked at any time through your device settings.

Permission	Why we request it	If you refuse
Location	To show Talents near you, to display distance and travel estimates, to pre-fill a service address, and to help detect fraudulent activity.	You can still search by entering a city or address manually.
Camera	To capture identity documents and liveness checks during verification, to upload portfolio images, and to attach evidence to a dispute.	You can upload existing images from your gallery instead.
Photo gallery	To upload a profile photograph, portfolio images, and evidence attachments.	You cannot upload images; some verification and dispute features will be unavailable.
Microphone	Only if you record or send a voice note through in-app messaging, or attach audio to a support request.	Text messaging remains fully available.
Notifications	To send booking confirmations, messages, payment updates, and security alerts.	You may miss time-sensitive booking and security information.
Contacts	Not currently used. If introduced in future, it would be requested separately and expressly for a referral feature.	No effect at present.

- 6.2** We collect precise location only while you are using the Platform, or in the limited circumstances disclosed to you at the time of the request. We do not track your location continuously in the background for advertising purposes.
- 6.3** Revoking a permission does not delete Personal Data already collected under that permission. To request deletion, see Clause 11.4.

7. Disclosure and Sharing of Personal Data

- 7.1** We do not sell Personal Data. We do not share Personal Data with third parties for their own independent advertising or cross-application tracking purposes.
- 7.2** We disclose Personal Data only as described below.

7.3 To other users

- 7.3.1** When a Booking is confirmed, we share with the Talent the Customer's name, contact number, service address, and the details of the Booking, so that the Service can be performed. We share with the Customer the Talent's name, profile, contact number, and verification status.

7.3.2 Before a Booking is confirmed, we share only limited profile information sufficient to enable discovery and communication. We do not disclose a Customer's exact address to a Talent before confirmation.

7.3.3 Your public profile, listings, ratings, and reviews are visible to other users of the Platform and may be visible to visitors who are not registered.

7.4 To service providers acting as Data Processors

7.4.1 We engage third parties to provide services on our behalf. They may process Personal Data only on our documented instructions, must maintain confidentiality and appropriate security, and must not use the data for their own purposes. Categories include:

- cloud hosting and storage providers;
- payment processing and payout providers;
- identity verification and document-authenticity providers;
- SMS, email and push-notification delivery providers;
- analytics and crash-reporting providers;
- customer support and ticketing platforms;
- fraud detection, sanctions screening and anti-money-laundering providers;
- professional advisers, including legal, accounting and audit firms.

7.4.2 A current list of our principal processors and sub-processors is available on request from [privacy@talinoo.com].

7.5 To authorities and for legal reasons

7.5.1 We disclose Personal Data to a Competent Authority where we are required to do so by Applicable Law, by a judicial order, or by a binding regulatory request, including to SDAIA, the Saudi Central Bank, the Zakat, Tax and Customs Authority, the Saudi Financial Intelligence Unit, and law enforcement bodies.

7.5.2 We also disclose Personal Data where necessary to: establish, exercise or defend a legal claim; prevent or investigate fraud, a crime, or a serious breach of our Terms and Conditions; or protect the vital interests, life, safety or health of any person.

7.5.3 Where we are legally permitted to do so, we will notify you of a request for your data. Where disclosure of the request is prohibited by law or would prejudice an investigation, we will not notify you.

7.6 Corporate transactions

7.6.1 If the Company is involved in a merger, acquisition, restructuring, or sale of assets, Personal Data may be transferred to the successor entity. We will notify you and ensure that the recipient is bound to protect your data on terms no less protective than this Policy.

8. Cookies, SDKs and Similar Technologies

8.1 On our website we use cookies. Within the mobile application we use software development kits (SDKs) and local storage that perform equivalent functions. We describe both here.

Category	Purpose	Consent
Strictly necessary	Authentication, session management, security, fraud prevention, load balancing, and remembering your language choice.	Not required — the Platform cannot function without these.

Category	Purpose	Consent
Functional	Remembering preferences, recently viewed listings, and saved search filters.	Consent required; may be withdrawn.
Analytics and performance	Understanding how the Platform is used, measuring feature adoption, and diagnosing crashes and errors.	Consent required; may be withdrawn.
Marketing and attribution	Measuring the effectiveness of campaigns and attributing installations to a campaign source.	Consent required; may be withdrawn.

8.2 We currently use, or may use, the following categories of third-party SDK. The specific providers in use at any time are disclosed within the application and in our app store privacy disclosures:

- Firebase (Google) — push notification delivery, remote configuration, and application analytics;
- Firebase Crashlytics (Google) — crash and stability reporting;
- a mobile analytics provider — product usage analytics;
- a payment provider SDK — secure collection of payment credentials;
- an identity verification SDK — document capture and liveness detection;
- an attribution provider — install attribution, where you have consented.

8.3 Each third-party provider processes data under its own privacy notice in addition to our instructions. Where a provider acts as an independent controller for any part of the processing, we identify this in our in-application disclosures.

8.4 Apple App Tracking Transparency

8.4.1 On iOS, we will not access your device’s advertising identifier (IDFA), and will not track you across applications or websites owned by other companies, unless you grant permission through Apple’s App Tracking Transparency prompt. If you decline, the Platform remains fully functional; only attribution and marketing measurement are affected.

8.5 Managing your choices

8.5.1 You can manage consent for non-essential cookies and SDKs at any time through the privacy settings within the application, through your browser settings for our website, and through your device settings for advertising identifiers and tracking. Withdrawing consent does not affect processing already carried out.

9. International Transfers of Personal Data

9.1 We host and process Personal Data primarily within the Kingdom of Saudi Arabia. Some of our service providers, however, operate infrastructure or support functions outside the Kingdom.

9.2 Where we transfer Personal Data outside the Kingdom, we do so only in the circumstances permitted by the PDPL and its Implementing Regulations, and in particular only where:

- the transfer serves the purposes set out in the PDPL, including the performance of a contract to which you are a party, the protection of vital interests, or compliance with a legal obligation or international agreement to which the Kingdom is a party;
- the transfer does not prejudice national security or the vital interests of the Kingdom;

- the destination jurisdiction provides an adequate level of protection as determined by the competent authority, or, in the absence of an adequacy determination, an appropriate safeguard is in place, such as standard contractual clauses, binding common rules, or an approved certification;
- we have conducted a risk assessment where one is required; and
- the transfer is limited to the minimum amount of data necessary.

9.3 You may request further information about the safeguards applied to a specific transfer by contacting us at [privacy@talinoo.com].

10. Retention of Personal Data

10.1 We retain Personal Data only for as long as necessary for the purpose for which it was collected, or for such longer period as is required by Applicable Law.

10.2 Our principal retention periods are set out below. Where a longer statutory period applies, the statutory period governs.

Data category	Retention period	Reason
Account and profile data	For the life of the account, then 12 months after closure	To allow reactivation and to resolve any residual dispute
Identity and verification records	10 years after the end of the relationship	Anti-money-laundering and know-your-customer record-keeping obligations
Booking and transaction records	10 years from the end of the relevant financial year	Commercial books, VAT and e-invoicing obligations
Payment and payout records	10 years from the end of the relevant financial year	Tax, VAT and accounting obligations
In-app messages	24 months after the related booking	Dispute resolution, trust and safety, and anti-circumvention
Support tickets and complaints	5 years after closure	Complaint handling and defence of claims
Ratings and reviews	Retained while the reviewed listing exists; may be retained in anonymised form thereafter	Integrity of the marketplace
Device, log and analytics data	12 to 26 months, depending on the dataset	Security, diagnostics, and product improvement
Records of permanently banned accounts	Indefinitely, in minimised form	To prevent the banned user creating a replacement account, and for safety

10.3 At the end of the applicable period, we securely delete Personal Data or irreversibly anonymise it so that it can no longer be attributed to you. Anonymised data may be retained and used indefinitely for statistical and product-improvement purposes.

10.4 Where data is held in encrypted backups, deletion from live systems takes effect immediately and the data is removed from backups in the ordinary backup rotation cycle.

11. Your Rights

11.1 Subject to the conditions and exceptions in the PDPL, you have the following rights in respect of your Personal Data.

11.2 Right to be informed

11.2.1 You have the right to know the legal basis and purpose for which your Personal Data is collected, and to be informed of any material change to this Policy. This Policy, together with in-application notices, satisfies that right.

11.3 Right of access and to obtain a copy

11.3.1 You have the right to request confirmation of whether we process your Personal Data, to access it, and to obtain a copy in a readable and clear format. The first copy is provided free of charge; we may charge a reasonable fee for additional copies where permitted.

11.4 Right to correction and to deletion

11.4.1 You have the right to request that inaccurate, incomplete or out-of-date data be corrected, completed or updated. Much of your data can be corrected directly in the application.

11.4.2 You have the right to request deletion of your Personal Data where it is no longer necessary for the purpose for which it was collected, where you withdraw consent and no other basis applies, or where the processing is unlawful.

11.4.3 We may decline a deletion request, in whole or in part, where retention is required by Applicable Law (for example, transaction records retained for tax and anti-money-laundering purposes), where the data is needed to establish, exercise or defend a legal claim, or where deletion would prejudice the rights of another user. Where we decline, we will explain why and will delete any part of the data not subject to the restriction.

11.5 Right to portability

11.5.1 You have the right to obtain the Personal Data you have provided to us in a structured, commonly used, machine-readable format, and to transmit it to another controller where technically feasible.

11.6 Right to object and to restrict processing

11.6.1 You have the right to object to processing carried out on the basis of legitimate interests, and to request restriction of processing while an objection or a correction request is being assessed. We will cease the processing unless we demonstrate compelling legitimate grounds that override your interests, or unless the processing is necessary for a legal claim.

11.7 Right to withdraw consent

11.7.1 Where we rely on consent, you may withdraw it at any time — for marketing, through the unsubscribe link or your notification preferences; for analytics and tracking, through the privacy settings in the application or your device settings. Withdrawal is as easy as giving consent, and does not affect the lawfulness of prior processing.

11.8 Rights relating to automated decisions

11.8.1 Where a decision producing a legal effect concerning you, or significantly affecting you, is taken solely by automated means, you have the right to request human review of that decision. See also Clause 12 and Clause 29.3.3 of the Terms and Conditions.

11.9 How to exercise your rights

11.9.1 Submit a request through the privacy settings in the application, or by writing to [privacy@talinoo.com] We may ask you to verify your identity before acting, in order to protect your data from unauthorised disclosure.

11.9.2 We will respond within thirty (30) days of receipt of a valid request. Where a request is complex or numerous, we may extend this period by a further thirty (30) days and will tell you if we do.

11.9.3 Exercising your rights is free of charge, unless a request is manifestly excessive or repetitive, in which case we may charge a reasonable fee or decline to act, and will explain our reasons.

11.10 Right to complain

11.10.1 If you are dissatisfied with how we have handled your Personal Data or your request, you may contact our Data Protection Officer at [privacy@talinoo.com]. You also have the right to lodge a complaint with SDAIA, the competent supervisory authority in the Kingdom of Saudi Arabia. We would appreciate the opportunity to resolve your concern first, but you are not required to contact us before approaching SDAIA.

12. Automated Processing and Artificial Intelligence

12.1 We use automated systems, including machine-learning models, for the purposes set out in Clause 29.3 of the Terms and Conditions. In summary, these are: ranking and recommending Talents and Services; matching Booking Requests; detecting fraud, circumvention, spam, fake reviews and prohibited content; assisting customer support; and generating translations and summaries.

12.2 Some of these systems process Personal Data. For example, our fraud-detection system analyses device, payment and behavioural signals; our content-moderation system analyses listings, reviews and messages for prohibited content and circumvention attempts.

12.3 Where an automated system produces a decision that significantly affects you — such as suspension of your account, withholding of a payout, or removal of a listing — you may request human review under Clause 11.8 and appeal under Clause 20.2 of the Terms and Conditions.

12.4 We do not use your Personal Data to train third-party artificial-intelligence models unless we have a lawful basis to do so and have disclosed that use in this Policy. Where we improve our own models, we use aggregated or anonymised data wherever technically possible.

13. Children's Privacy

13.1 The Platform is intended solely for persons aged eighteen (18) years or older. We do not knowingly collect Personal Data from any person under that age.

13.2 If we become aware that we have collected Personal Data from a person under eighteen, we will suspend the account immediately and delete the data without undue delay, except where retention is required by Applicable Law.

13.3 If you believe that a person under eighteen has provided Personal Data to us, or that a minor is using the Platform, please contact us immediately at [privacy@talinoo.com].

13.4 Where a Customer books a Service that will be received by or performed in the presence of a minor, the Customer is the account holder and is responsible for the minor. Any information about the minor provided in a Booking (for example, a child's age or allergy for an event) is provided by the adult Customer, is minimised to what is necessary for the Service, and is deleted in accordance with Clause 10.

14. Security of Personal Data

14.1 We implement technical, organisational and administrative measures appropriate to the risk, including:

- encryption of data in transit using TLS, and encryption of data at rest;
- hashing and salting of passwords, which are never stored in plain text;
- role-based access controls, applying the principle of least privilege, with access logging;
- multi-factor authentication for administrative and privileged access;
- network segmentation, firewalls, and intrusion detection;
- tokenisation of payment credentials by our licensed Payment Providers, so that full card numbers are not stored on our systems;
- regular vulnerability scanning, patch management, and periodic penetration testing;
- secure development practices, code review, and dependency monitoring;
- confidentiality undertakings and data protection training for personnel;
- due diligence and contractual safeguards for processors;
- encrypted backups and a documented disaster recovery plan.

14.2 No system is completely secure. While we take these measures seriously, we cannot guarantee absolute security, and you are responsible for keeping your account credentials confidential, in accordance with Clause 5.3 of the Terms and Conditions.**14.3 Incident response and breach notification****14.3.1** We maintain a documented incident response procedure covering detection, containment, assessment, notification and remediation.**14.3.2** Where a personal data breach occurs, we will notify SDAIA within the period required by the PDPL and its Implementing Regulations, being no later than seventy-two (72) hours from becoming aware of the breach where the breach may cause harm to personal data or to the data subject.**14.3.3** Where the breach is likely to cause serious harm to you, we will notify you without undue delay, describing the nature of the breach, the likely consequences, the measures taken, and the steps you can take to protect yourself.**15. App Store Privacy Disclosures****15.1** This Clause is provided so that our disclosures on the Apple App Store and Google Play are consistent with this Policy. In the event of any inconsistency, this Policy governs, and we will correct the store disclosure.**15.2 Apple App Store — privacy label summary**

Label category	Data types	Use
Data used to track you	Advertising identifier, usage data — only with your ATT permission	Attribution and campaign measurement
Data linked to you	Contact info, identifiers, financial info, location, user content, usage data, diagnostics	App functionality, verification, payments, safety, support
Data not linked to you	Aggregated diagnostics and crash data	Stability and performance

15.3 Google Play — Data Safety summary

Disclosure	Position	Notes
Data collected	Yes	Categories as described in Clause 4
Data shared	Yes	With processors, payment providers, and authorities — see Clause 7
Data encrypted in transit	Yes	TLS
Deletion request mechanism	Yes	In-app and via the privacy email — see Clause 11.4
Committed to Play Families Policy	Not applicable	The app is rated for adults 18+

15.4 Account and data deletion route

15.4.1 In accordance with Google Play's account deletion requirements and Apple's App Store Review Guidelines, you can request deletion of your account and associated data from within the application. Deletion is subject to the statutory retention exceptions in Clause 11.4.3.

16. Changes to this Policy

16.1 We may update this Policy to reflect a change in our processing activities, in the Platform, or in Applicable Law.

16.2 Where a change is material — for example, a new purpose of processing, a new category of recipient, or a change to retention — we will notify you in advance through the Platform, by email, or by in-application notice, and where the change requires your consent we will obtain it before the change takes effect.

16.3 The "Last Updated" date on the cover page indicates when this Policy was last revised. We maintain previous versions and will provide a copy on request.

17. Contact Us

For any question about this Policy, or to exercise any of your rights, please contact us.

Matter	Contact
Company legal name	Bayata Company for Information Technology
Registered address	7033191102
Registered address	Damman Rd., Al Yarmuk Dist. Riyadh, Postal Code: 13251
Data Protection Officer	privacy@talinoo.com
Privacy and data protection	privacy@talinoo.com
General support	support@talinoo.com
Legal and regulatory	support@talinoo.com
Telephone	+966 552527631
Website	www.talinoo.com
Supervisory authority	Saudi Data and Artificial Intelligence Authority (SDAIA)

END OF PRIVACY POLICY