



Privacy Policy

Version 2.0: effective 17 September 2026 for members who join on or after that date, and from 17 October 2026 for members who joined earlier ·
replaces the Privacy Policy effective 1 August 2026 (revised 31 August 2026)
· last reviewed 17 September 2026

Nu Pare Pty Ltd · ACN 698 123 545 · 143 St Georges Terrace, Perth WA 6000, Australia
hello@nupare.com.au · nupare.com.au/legal

N U P A R E

Contents

Summary.....	4
1. Who is responsible, and how to reach us.....	4
2. Information we collect.....	4
3. Why we use your information, and on what legal basis.....	7
4. Automated decisions, profiling and AI.....	11
5. Who we share information with.....	12
6. Where your information goes.....	13
7. How we protect information.....	14
8. How long we keep information.....	14
9. Your rights.....	16
10. Marketing and communications.....	17
11. Cookies, SDKs and tracking.....	18
12. Children.....	18
13. Data breaches.....	18
14. Changes to this Policy.....	19
15. Complaints.....	19
16. Business contacts.....	19
17. Definitions.....	19
Regional Annexes.....	20
Annex A: Australia.....	20
Annex B: New Zealand.....	21
Annex C: United Kingdom.....	22
Annex D: European Economic Area (and Switzerland).....	22
Annex E: United States.....	24
Annex F: Canada.....	26
Annex G: Singapore.....	27
Annex H: Japan.....	28
Annex I: Hong Kong.....	29
Annex J: Republic of Korea.....	29
Annex K: Malaysia.....	31
Annex L: United Arab Emirates.....	31
Annex M: Kingdom of Saudi Arabia.....	31
Further Annexes.....	33
Annex N: Cookie and Tracking Policy.....	33
N.1 What this Annex covers.....	33
N.2 The four categories.....	33
N.3 The register.....	34
N.4 How consent works where you live.....	35
N.5 How to control tracking.....	37
N.6 Do Not Track.....	37
N.7 Changes.....	37
Annex O: Sub-processors.....	37

Annex P, Korea: 개인정보 처리위탁 및 국외이전 현황 (nupare.com.au/kr/entrustment · nupare.com.au/kr/transfer).....	39
Annex Q, Japan: 外国における個人情報の保護に関する制度 (nupare.com.au/jp/kaigai).....	40
Annex R: Biometric Data Retention and Destruction Policy (United States), nupare.com.au/legal/biometrics.....	41
Separately published notice.....	42
Consumer Health Data Privacy Policy (Washington, Nevada, Connecticut): nupare.com.au/legal/consumer-health-data.....	42

Summary

We collect the information you give us (including what you add to your digital wardrobe from photos, receipts and connected email), the information your use of the app generates (including a record of the screens you visit and what you tap, kept for 30 days), and some information from others (such as Stripe and, if you are referred, the person who referred you). We use it to run the marketplace, Resale, subscription, Points, Creator, booking, wardrobe, styling and community features; to keep the platform safe; to meet legal duties such as Seller verification and tax reporting; and, with your permission where the law requires it, to personalise your experience and send you marketing. We store it in Australia (Sydney). Images you use for virtual try-on are processed in the United States. We do not sell it. You can access, correct, delete and take a copy of it, object to and opt out of some uses, and complain to us and to your privacy regulator. Sections 1 to 16 set out the detail; the Regional Annexes at the end state what differs where you live.

1. Who is responsible, and how to reach us

1.1 Controller. Nu Pare Pty Ltd, ACN 698 123 545, of 143 St Georges Terrace, Perth WA 6000, Australia (**NuPARE, we, us**) is the controller of the personal information described in this Policy: you can reach us at privacy@nupare.com.au or by post at that address.

1.2 Privacy Officer and Data Protection Officer. You can reach our Privacy Officer (who is also our Data Protection Officer for the purposes of the laws that require one, including in Singapore, Malaysia and the EEA) at privacy@nupare.com.au and by post marked "Privacy Officer". We publish their name and title on our Legal Contacts page at nupare.com.au/legal/contacts.

1.3 Representatives. Because we are established in Australia, we are required to appoint representatives in the European Union (under Article 27 of the GDPR) and the United Kingdom (under Article 27 of the UK GDPR). We publish their names and postal addresses on the Legal Contacts page and in Annexes C and D; we do not offer the Service in the EEA or the United Kingdom until those particulars are published there. You may contact them on any matter relating to this Policy. Where the law of another country requires a local representative, the Legal Contacts page names them.

1.4 Others who are responsible for their own use. Stripe, our payment services provider, is independently responsible for the payment information it processes and for the identity and financial information it collects to open your connected account; its privacy policy is linked at checkout and in Settings > Payments. Brand Partners are independently responsible for the information they receive to fulfil your order, to answer your messages and to see you as their customer (section 5.5), within the limits our agreement with them sets. Sellers, Stylists and Care Providers who receive your name and address to fulfil an order or booking are responsible for their own use of it, and our terms with them limit that use to the transaction.

2. Information we collect

2.1 Information you give us.

Category	Examples	When
Identity and contact	Name, handle, email, mobile number, date of birth, delivery and billing addresses, profile photo; and, if	Account creation; checkout; profile

Category	Examples	When
	you choose to give them, gender, pronouns and who you shop for	
Wardrobe	Photographs of your pieces and receipts, care labels, screenshots, pasted text and links you add; piece details imported from them (brand, item, size, price, date, retailer); valuations; the evidence (subject line and date of a receipt email) we keep for each piece	When you digitise your wardrobe
Email you forward or connect	Raw email you forward to your personal NuPARE address (kept for 30 days) and, if you connect Gmail or Outlook, the receipts we read from those mailboxes under the permission you grant (Google's Limited Use requirements apply to Gmail data, as section 3 explains)	When you forward or connect email
Calendar	Event titles, times and places, if you grant calendar access, used to suggest outfits for what is coming up	If you grant the permission
Body and fit	Measurements you enter; a photograph of yourself, if you choose to use it for virtual try-on; a body figure generated from your measurements	If you use fit or try-on features
Style profile	Your style identity, the "learned" preferences the AI stylist keeps (which you can view and delete), outfits and capsules you save	When you use the AI stylist
Verification	Business registration, ABN and tax identification numbers, bank account details (collected by Stripe), producer or packaging registration numbers, and, where the law of your country requires it for Sellers or Providers, a government-issued identity document (and a selfie for identity matching where you choose that method)	When you sell, provide services, join the Creator Program, or the law requires it
Transaction	Items bought and sold, prices, fees, delivery details, returns, disputes, Resale Protection claims	Every transaction
Bookings	Provider chosen, service, time, location of an in-person session, piece declared value and condition photos, complaints	Provider bookings
Preferences	Sizes, measurements you enter, style preferences, brands followed, wishlists, saved searches	If you choose to enter them
Content	Listings, photographs, descriptions, reviews, posts, polls, stories, live chat, Creator content, reads, episodes, direct messages and attachments to other members, and messages to Brand Partners and to us	When you post or send them
Community	Circles you run or join, gatherings you organise or attend, tickets and transfers, votes	When you use those features
Voice	Audio of a voice search, converted to text on the device by Apple's speech recognition; we receive the text	When you use voice search
Partner access grants	The scope and duration of access you grant a partner Stylist to your wardrobe, and the audit record of each time they looked (or were refused)	When you grant access
Support	Correspondence, complaints, appeals, survey responses	When you contact us
Criminal history	Result of a criminal-history check, where you are a Stylist offering in-person sessions and you consent	Stylist onboarding, where lawful

2.2 Information we collect automatically.

Category	Examples
Device and app	Device type, operating system, app version, language, time zone, push token, device registry entry, crash and performance reports (collected

Category	Examples
Screen and tap trail	through Apple's MetricKit and sent to us; kept for 90 days), IP address The screens you visit and the controls you tap in the app, batched about every 30 seconds and kept for 30 days, so we can reproduce problems and understand how features are used; it is erased with your account. In countries where the law requires consent for this kind of collection it runs only with your consent (Annex N)
App analytics	Firebase Analytics events (screens viewed, features used), on by default and switchable off at Settings > Privacy > Analytics; in countries that require consent it is off until you turn it on
Presence	Whether you are online, shown to members you follow and who follow you (switchable off)
Experiments	Which version of a feature you were shown when we test changes
Usage	Pages and items viewed, searches, taps, time spent, referral links used, features used
Location	Approximate location derived from IP address (always); device location only while you use a feature that needs it (the weather for outfit suggestions, or finding nearby Providers), and not stored
Transaction security	Signals used to detect fraud, such as device fingerprint, velocity of activity and payment-risk indicators
Cookies and similar technologies	See Annex N

2.3 Information we collect from others. Some countries (including New Zealand, from 1 May 2026) require us to tell you specifically when we collect information about you from someone other than you. We collect: your name, address and contact details **from a Seller or Provider** when they dispatch to you or complete a booking; your contact details **from a member who refers you** (we tell you at first contact that we received them from that member, why, and how to have them deleted); payment results, payment-risk scores and connected-account status **from Stripe**; receipts and order emails **from Gmail or Outlook** if you connect them, and from retailers who email your NuPARE forwarding address; sign-in information **from Apple or Google** if you sign in with them (name, email, and an identifier); order and shipment updates **from Brand Partners and their systems** (Shopify, WooCommerce, BigCommerce) and tracking events **from Australia Post and AfterShip**; click and sale records **from the affiliate networks** (Awin, Rakuten Advertising, Commission Factory, Impact) for Creator attribution (click tokens, not your identity); analytics and attribution data **from the analytics and advertising partners** named in Annex N; business registration, VAT and sanctions-screening results **from public registers and screening providers** when you sell or provide services; and reports about you **from other members, rights holders, trusted flaggers, regulators and law enforcement**. We do not buy personal information from data brokers.

2.4 Sensitive information. We collect device location only for the feature you are using and do not store it. Calendar access, if you grant it, reads event titles, times and places only to suggest outfits, and we do not keep the events beyond the suggestion. A photograph you use for virtual try-on is used only to generate an image of you wearing a piece. We do not use it to identify or authenticate you, create, store or compare a face- or body-geometry template from it, or use it for facial recognition or facial analysis; it is not "biometric data" under Article 4(14) of the GDPR or the UK GDPR, which require processing directed at unique identification. Where you live in a state whose biometric law applies to a scan of face or body geometry regardless of purpose (including Illinois, Texas, Washington and Colorado), we treat the image as covered by Annex E.11. Before we process it we give you

the separate written notice and obtain the written release that Annex describes. We delete the image and anything derived from it when the try-on is complete, and we do not sell, lease, trade or otherwise profit from it. Our retention and destruction schedule is in Annex R. Our image-generation providers are contractually prohibited from retaining the image, deriving a template from it, or using it for any purpose other than generating your try-on image. We collect a criminal-history result only for Stylists who consent, where lawful. We collect a facial image for identity matching only if you choose that verification method, and the biometric template is held by our verification vendor, not by us, and deleted within 30 days of verification. In Australia a facial image used for identity matching is sensitive information and we collect it only with your express consent, and only where it is reasonably necessary for a verification the law requires. We collect government identity documents only where the law requires Seller or Provider verification. We do not ask for, and ask you not to post, information about your health, religion, ethnicity, sexual orientation or political views; if you include it in content or measurements (for example maternity or adaptive sizing), we use it only to provide the feature you are using and it is covered by Annex E.10 where you live in Washington or Nevada. We do not use special-category or sensitive information for advertising or profiling.

2.5 If you do not provide information. You cannot create an account without a name, email address and age confirmation; you cannot buy without a delivery address and payment method; you cannot sell, provide services or earn commission without the verification information the law requires (and if you do not provide it we must suspend those activities and, in some countries, withhold payouts). Everything else is optional and we tell you so when we ask.

2.6 App permissions. The app asks for these permissions, each for the purpose stated and each optional: Photos (to add pieces and receipts to your wardrobe and to post); Camera (to photograph pieces, receipts and care labels, to post, and to broadcast live); Microphone (voice search and live broadcasts); Speech recognition (voice search, processed on your device); Location when in use (the weather for outfit suggestions and nearby Providers; not stored); Calendar (outfit suggestions for upcoming events); Notifications (order, booking, message and safety alerts, and marketing only if you opt in). You can change any permission in your device settings; the feature that needs it will not work without it, and nothing else is affected.

3. Why we use your information, and on what legal basis

Where the law of your country requires a legal basis for each use (as in the EEA, the UK, Switzerland, Korea, Singapore and elsewhere), this table states it. "Contract" means the use is necessary to perform our contract with you; "legal obligation" means a law requires it; "legitimate interests" means the use is necessary for our or a third party's legitimate interests, which are stated, and we have assessed that your interests do not override them (you can ask us for a copy of that assessment); "consent" means we ask you first and you can withdraw at any time.

Purpose	What we do	Legal basis
Providing the Service	Create and run your account; show listings; process orders, payments, deliveries and returns; run Insider and Points; take and manage bookings; send transactional messages	Contract
Payments,	Verify identity, age and payout details;	Legal obligation (anti-money-laundering,

Purpose	What we do	Legal basis
verification and fraud prevention	screen against sanctions lists; detect and prevent fraud, scams, account takeover and chargeback abuse; hold payouts where we reasonably suspect fraud	sanctions, marketplace-verification and age laws); legitimate interests (protecting members and NuPARE from fraud); contract
Seller, Provider and Creator verification and publication	Collect and verify the information in clause 5.11 of the Terms; publish a business Seller's name, address and contact details on their listings where the law requires; disclose a Seller's identity to a buyer with a claim	Legal obligation (Digital Services Act Art 30; INFORM Consumers Act; Japan's Digital Platform Consumers Act; Malaysia's e-commerce regulations; Korea's E-Commerce Act; consumer laws generally)
Tax reporting and withholding	Report Seller and Provider identity and income to tax authorities; withhold tax where required; collect and remit sales tax, VAT and GST	Legal obligation (DAC7 and the platform-reporting laws of the UK, Australia, New Zealand and Canada; US Form 1099-K; marketplace-facilitator and deemed-supplier laws)
Resale Protection, Provider complaints and disputes	Review evidence, decide claims, hold and release funds, handle appeals	Contract; legitimate interests (fair operation of the marketplace)
In-person session safety	Share an address with a Stylist only after confirmation; keep a record of in-person bookings; act on safety reports	Contract; legitimate interests (safety of members and Providers); legal obligation where a report must be made
Safety, moderation and enforcement	Screen listings, images, messages and reviews with automated tools and human review; act on reports; suspend and terminate accounts; give statements of reasons; keep records for appeals and transparency reports	Legal obligation (Digital Services Act; Online Safety Acts of the UK, Australia, Singapore and Malaysia; product-safety and consumer laws); legitimate interests (keeping the Service safe and lawful)
Product safety and recalls	Identify and contact buyers of a recalled or unsafe item; publish recall notices; report incidents to regulators	Legal obligation (General Product Safety Regulation; consumer product safety laws)
Points and Insider	Calculate, credit, expire and redeem Points; provide Insider benefits; send reminders	Contract; in California, Annex E.6 (notice of financial incentive)
Creator attribution and payment	Track purchases attributed to a Creator's links and content; calculate and pay commission; detect fraudulent attribution	Contract (with the Creator); legitimate interests (operating the Creator Program, preventing fraud); consent where cookies or identifiers are used for attribution in countries that require it
Personalisation	Rank and recommend items, Providers and content based on your activity; remember preferences	Legitimate interests (a relevant experience), with the ability to turn personalised ranking off in Settings > Personalisation; consent where your country's law requires it for profiling
Marketing	Send you email, push and SMS about NuPARE, Brand Partners' items and offers; show you NuPARE advertising on other platforms; measure campaigns	Consent where the law requires it; legitimate interests (marketing our own similar products to existing customers) where the "soft opt-in" in regulation 22 of the UK Privacy and Electronic Communications Regulations or an equivalent national rule applies, with an opt-out at collection and in every message; legitimate interests for measurement
Analytics and improvement	Understand how the Service is used; fix bugs; test features; train and evaluate our fraud, search, sizing and moderation models	Consent, where the law of your country requires consent to store or read information on your device for this purpose; otherwise legitimate interests

Purpose	What we do	Legal basis
		(improving the Service)
Criminal-history checks for Stylists	Obtain and record the result of a criminal-history check on a Stylist who offers in-person sessions	Consent and, in the EEA and the United Kingdom, only where the law of your country expressly authorises a check for this activity and provides appropriate safeguards (Article 10 of the GDPR, as Annex D.13 explains); legitimate interests (the safety of members)
AI features	Provide AI search, styling suggestions, size recommendations, listing assistance and support assistants	Contract (the feature you use); legitimate interests (improving the feature), as section 4 explains
Communicating with you	Respond to enquiries, complaints and requests; send service notices and changes to terms	Contract; legal obligation
Digital wardrobe	Read the photos, receipts, screenshots, links and emails you add or connect; import piece details with AI (Claude on Amazon Bedrock, in Australia); value pieces; keep evidence. Gmail data is used only to identify and record purchases in your wardrobe, is never used for advertising, is not sold, and is not read by a person except with your consent, for security, or to comply with law, in accordance with Google's API Services User Data Policy, including its Limited Use requirements	Contract (the feature you use); consent (the mailbox permission you grant)
Face and body features	Where a feature works on the shape of you rather than of a piece (a try-on render on your own body, or a fit estimate from a photograph of you), we ask for your express, opt-in consent before it runs for the first time, in every country , tell you what is collected and for how long, and never turn it on by default. You can withdraw consent at any time in Settings and we delete the underlying facial or body data. Where a United States biometric statute applies we also take the separate written release it requires	Consent (and, in Australia, Australian Privacy Principle 3.3)
Rewards	Confirmed eligible spend over the trailing 12 months, tier and tier history, benefit year, care allowance issued, reserved and claimed, and invitation assessments, to run the Rewards programme. Noir invitations use documented commercial criteria and human review, and never a sensitive attribute	Contract
Styling services	Appointment bookings, the brief you give, preparation notes, the action plan produced for you and coordinator correspondence, to deliver the reviews and appointments in Parts 6 and 7 of the Terms	Contract
Paid gatherings and circles	Host and founder payout records, ticket and subscriber billing records, and the identity and income information we must	Contract; legal obligation

Purpose	What we do	Legal basis
	report for them	
Care Promise claims	The claim file, the value you declared and the custody photographs, shared with the Provider and, where we recover under an assigned claim, with the Provider's insurer	Contract; our legitimate interest in recovering what we have paid
Acceptance record	The version of the Terms you accepted, the date and time, and the country we identified you in, as evidence of the contract	Legal obligation; our legitimate interest in being able to prove the agreement
Mailbox connection	Where you connect a Google or Microsoft mailbox, read messages that appear to be purchase confirmations or receipts and import the seller, order reference, pieces, sizes, colours, quantities, purchase prices, currency and dates, to draft entries for your wardrobe. An imported detail is identified, not confirmed: no entry joins your wardrobe until you have reviewed and accepted it. We do not read, store or index the rest of your mail, and we never use anything from it for advertising. We delete the import records within 30 days of you disconnecting, unless a transaction, tax or dispute record requires a line to be kept; every human access to your mail is logged and is permitted only where you asked us to look, where you gave express consent, where security or an abuse investigation requires it, or where the law requires it; and information about the people who wrote to you is never profiled, imported or disclosed for anyone else's purposes. Part 12B of the Terms sets out the limits, including the provider limited-use rules we are bound by	Consent
Images we generate	Create cutouts, drawn replicas, try-on renders and Passport imagery from the photographs you upload, and hold them as part of your wardrobe. We do not use your photographs, the images generated from them, or your wardrobe records to train general-purpose or foundation models	Contract; consent for anything using your face or body
Virtual try-on	Generate an image of you (from your photograph, or a body built from your measurements, or a standard body we tell you is not yours) wearing a piece, using image models run by Stability AI (United States) and OpenAI (United States); piece drawings by Google Gemini; body figures cached so you need not re-upload	Contract; consent for the use of your photograph
AI stylist and search	Answer questions, suggest outfits, weeks and capsules, and keep a "learned" memory you can edit or delete, using Claude on Amazon	Contract; legitimate interests (improving the feature)

Purpose	What we do	Legal basis
	Bedrock (Australia and Asia-Pacific regions), Amazon Titan embeddings, and Brave Search for grounding	
Community features	Run direct messages, brand messages, stories, live broadcasts (not recorded), circles, reads, episodes, gatherings and tickets	Contract
Digital Passport	Build and maintain a record of a piece from what you and the seller enter, from purchase and order records, and from images you upload; carry that record with the piece on resale; and show buyers what is recorded and what is not. We do not physically examine or authenticate pieces	Contract; legitimate interests (marketplace integrity)
Experiments and research	Show different versions of a feature to different members and measure the result	Legitimate interests (improving the Service); consent where required
Partner Stylist access	Let a Stylist you choose read your wardrobe within the scope and time you grant, and log every access	Consent (your grant)
Legal and corporate	Establish, exercise or defend legal claims; comply with court orders, regulators and law enforcement; audit; insurance; a merger, acquisition or reorganisation	Legal obligation; legitimate interests (protecting our rights; running our business)

We do not use your personal information to set individualised prices. We do not sell your personal information for money. We do not share it with Brand Partners or Creators for their own marketing without your separate consent.

4. Automated decisions, profiling and AI

3.9A The analytics beacon and cookies. Every page on nupare.com.au loads a small analytics beacon that records the page, the referrer, the user agent and an approximate location derived from the network address, whether or not you have an account. We use it to understand how the site is used and to keep it working. Where the law of your country requires consent before a non-essential cookie or similar technology is set, we ask for it through a consent banner before setting one, we set only strictly necessary cookies until you answer, and we make refusing as easy as accepting. Annex N is our Cookie and Tracking Policy and lists what is set, by whom and for how long.

4.1 Decisions made entirely by automated means. The following decisions can be made by our systems without a person: blocking a payment or listing that matches a high-confidence fraud or prohibited-item signal; placing a temporary hold on a payout pending review; removing content that matches known illegal material; crediting, expiring and adjusting Points; attributing a purchase to a Creator; personalised ranking; size and fit recommendations; AI stylist outfit suggestions; Smart Pricing adjustments to a Resale price where you have opted in; rate limits; and releasing a Resale payment when the claim window closes without a claim. These use your transaction history, device and usage signals, listing and message content, and (for attribution) link and cookie data. They can affect your access to funds, your ability to sell or post, and what you see. In every case you can ask for a person to review the decision (section 9.6), we tell you when the decision

affects you, and we do not base any such decision on special-category or sensitive information.

4.2 Decisions where automation assists a person. Account suspension and termination, Resale Protection and Provider complaint outcomes, Creator commission reversals, reclassification of a Seller as a business, moderation of reported content, and appeals are decided by a person using information and recommendations produced by our systems.

4.3 Profiling. We build a profile of your preferences from your activity to personalise ranking and recommendations, and, with consent where required, for marketing. The main parameters, and how to turn personalised ranking off, are in the Terms (clause 3.9). We do not profile for advertising anyone we know to be under 18, and we do not use special categories of data in profiling.

4.4 AI features. Our AI features use the information you give the feature (a search query, a photo of a piece for a listing, your measurements) and, for recommendations, your activity. We do not store outputs beyond what is needed to provide the feature and improve it. We do not use your photographs, messages or content to train generative AI models, other than to evaluate and improve the specific feature you used them with, and we do not share them with model providers for their own training. Where an AI feature interacts with you directly, we tell you it is automated.

4.5 Regional rules. Annexes A (Australia, from 10 December 2026), C (UK), D (EEA), E (California, from 1 January 2027), F (Quebec) and J (Korea) set out additional rights and disclosures about automated decisions where you live.

5. Who we share information with

5.1 Other members, to complete a transaction. Your name and delivery address go to the Seller of an item you buy; a buyer's name and address go to you when you sell; your name, the service booked and, for in-person sessions, the session address go to a Provider after the booking is confirmed. Members must use that information only for the transaction. Your handle, profile photo, reviews, listings, looks, posts, reads, episodes and Creator content are visible to other members and, unless your account is private, to the public and to search engines; stories are visible to the audience you choose; live broadcasts are visible to those who join; circle Organisers see who is in their circle; gathering Organisers receive ticket holders' names; your presence is shown to members you follow and who follow you unless you turn it off. A partner Stylist you grant access to sees the parts of your wardrobe you allow, for the time you allow, and you can see every time they looked.

5.2 Published Seller information. Where the law requires (currently the EEA under the Digital Services Act, the United States under the INFORM Consumers Act for high-volume Sellers, and countries whose consumer laws require trader identification), we publish a business Seller's name, address, contact details and registration numbers on their listings. Where the law requires, we disclose a Seller's or Provider's identity, address and phone number to a buyer or customer who has a claim against them (for example in Japan and Korea).

5.3 Service providers (processors). We use providers to host and run the Service, process payments and verify identity, deliver items, send email, push and SMS, provide customer-support tools, analytics, fraud detection, content moderation, and professional advice. They act on our instructions under written contracts that require them to protect your information

and use it only for our purposes. The current list of categories and, for the principal providers, names and locations, is in Annex O.

5.4 Payment provider. Stripe receives the information needed to process payments and to open and verify a connected account for Sellers, Providers, Creators and Organisers, and is independently responsible for that.

5.5 Brand Partners. A Brand Partner receives your name, delivery address and order details to fulfil an order you place with it, and your messages when you message it. A Brand Partner can also see, for its own customers, your name, handle, suburb and state, number of orders, spend, units and first and last order dates, so it can serve you; on the Index plan it also sees aggregated wardrobe insights that do not identify anyone. A Brand Partner may use this information only to fulfil and service your orders and, under the data-sharing terms of our agreement, may not use it to market to you unless you consent separately, and must delete it when it is no longer needed for those purposes.

5.6 Tax authorities, regulators and law enforcement. We disclose Seller and Provider information to tax authorities as section 3 describes; we respond to lawful requests from courts, regulators, police and safety authorities; and we report suspected stolen goods, fraud, child safety matters and product-safety incidents where the law requires or permits.

5.7 Rights holders. If you list an item that is the subject of an infringement notice, we may disclose your name and contact details to the rights holder where the law requires or a court orders it.

5.8 Corporate transactions. If we sell or reorganise our business, your information may be transferred to the successor, who must honour this Policy; we tell you before that happens and you may close your account.

5.9 With your consent. We share your information in any other case only with your consent.

6. Where your information goes

6.1 Locations. We are based in Australia and our systems run in Amazon Web Services' Sydney region (Australia), including the text models we use (Claude on Amazon Bedrock). We ask for Australian and Asia-Pacific endpoints wherever the provider offers them, and we tell you that some model identifiers are cross-region: where a request is served outside Australia we rely on the safeguards in section 6.2, and we do not represent that every text request is processed only in Australia. Photographs and body figures used for virtual try-on and for the images we generate are **generated**, not merely analysed, outside Australia: they are processed in the United States by Stability AI in Oregon and by OpenAI, and by Google (Gemini), and are cached in the United States. Generating an image from your photograph creates and stores a new image, which is a more substantial use than analysis, and we describe it that way so that you can assess it. Part 12A of the Terms explains what those images are and who owns them. Other providers process information in the United States and, depending on the provider, the European Union, the United Kingdom, Singapore and Japan: Stripe (payments), Google (Firebase Analytics, website analytics, Gmail connection, sign-in), Microsoft (Outlook connection, Teams invitations for Stylist sessions), Apple (push notifications, sign-in), Australia Post and AfterShip (tracking), Brave (search grounding for AI answers), the affiliate networks (click tokens only), and our support and email providers. Information also goes to the country where a member, Brand Partner or Provider you transact with is located. The current list is in Annex O.

6.2 Safeguards. Where information is transferred from a country whose law restricts transfers, we use the mechanism that law recognises: for the EEA, the European Commission's standard contractual clauses (2021) with a documented transfer impact assessment, and, for United States providers certified under the EU-US Data Privacy Framework for the relevant data, that Framework, with the clauses as a fallback; for the UK, the International Data Transfer Agreement or the UK Addendum, with a transfer risk assessment, and the UK Extension to the Data Privacy Framework where available; for Switzerland, the clauses with the Swiss amendments; for Australia, the steps required by Australian Privacy Principle 8; for New Zealand, the requirements of Information Privacy Principle 12; for Singapore and Malaysia, contractual obligations providing a comparable standard of protection; for Japan and Korea, the information and consents in Annexes H and J; for Saudi Arabia, the standard contractual clauses approved by the Saudi Data and Artificial Intelligence Authority with a risk assessment; and for Quebec, a privacy impact assessment and written agreement under section 17 of the Act respecting the protection of personal information in the private sector. You can ask us for a copy of the relevant safeguards at privacy@nupare.com.au.

6.3 Government access. Information stored in another country may be accessible to the courts, law enforcement and national security authorities of that country under its laws. We assess that risk in our transfer assessments and we challenge requests that we consider unlawful or over-broad.

7. How we protect information

We protect your information with organisational measures (a designated Privacy Officer, staff confidentiality obligations, role-based access, privacy and security training, vendor due diligence, incident-response and business-continuity plans); human measures (background screening of staff with access to verification data, and access reviews); physical measures (data centres with certified physical security, no verification documents held on paper); technical measures (encryption in transit and at rest, multi-factor authentication for staff, logging and monitoring, vulnerability management and penetration testing, segregation of verification and payment data, and automated deletion at the end of retention periods for most records, with manual review and purge where automation is not yet in place, as the Data Retention Schedule sets out); and, for information handled in a foreign country, an assessment of that country's legal environment and contractual safeguards with the provider. No system, and no transmission over the internet, is perfectly secure, and we cannot guarantee the security of information you choose to publish on the Service or send to another member, a Brand Partner or a Provider, or of a device, network or email account that you control. We ask you to keep your login details safe, to use the security features we offer, and to tell us at once if you think your account has been compromised. This paragraph describes the limits of what any provider can promise; it does not reduce our obligations under the privacy or consumer law of your country, or our liability under clause 15.2 of the Terms of Service.

8. How long we keep information

We keep information for as long as needed for the purpose we collected it, and then for as long as the law requires. The main periods are:

Information	Period	Why
Account and profile	While your account is open; on	To let you reopen the account;

Information	Period	Why
	deletion, a 30-day grace period in which you can reopen it, then erasure of everything except orders, payment and tax records	then deleted
Transactions, invoices, payouts	7 years from the transaction	Tax and accounting laws (Australia 5–7 years; EEA up to 10 years in some Member States; Canada 6 years)
Seller and Provider verification data	While you sell or provide services, then 5 years after your last transaction	Anti-money-laundering, marketplace-verification and tax-reporting laws; product-safety record-keeping (Canada 6 years)
Identity documents	Deleted within 30 days of verification; a record of the result and document type is kept with the verification data	Data minimisation
Tax reports	7 years from the report	Tax laws
Content, listings, reviews	While published and for 90 days after removal (longer if subject to a dispute or legal hold)	Appeals; transparency reporting
Generated images (cutouts, drawn replicas, try-on renders, Passport imagery)	Until you delete the source photograph or the item they are attached to (Terms clause 12A.7)	Your wardrobe, looks and Passports
Care custody photographs	12 months from the return of the piece	Evidence of condition on arrival and return
Piece day index	400 days	Wardrobe insights and wear tracking
Brand feed files	31 days	Catalogue ingestion and troubleshooting
Marketing suppression list	Indefinitely, as a hashed email address only	So we do not contact you again after you opt out
Transfer and privacy impact assessments	5 years after supersession	Accountability and regulator inquiries
Contracts with Brand Partners, Providers and vendors	7 years	Legal and tax records
Acceptance record (version accepted, date and time, country identified)	While your account is open and 7 years afterwards; it survives account erasure	Evidence of the contract
Connected-mailbox import records and access tokens	30 days after you disconnect, unless a transaction, tax or dispute record requires a line to be kept	Building your wardrobe from receipts
Messages, stories, posts, comments	Until you delete them or your account is erased; a story leaves view after 24 hours and is deleted 7 days later; safety-investigation copies for 3 years	Resale Protection, safety investigations, dispute evidence

Where this table and the Data Retention Schedule in the Platform Policies differ, the shorter period applies.

Screen and tap trail	30 days	Diagnostics and product improvement
Forwarded email (raw)	30 days	Wardrobe import
Imported wardrobe evidence (subject, date,	Life of the piece in your wardrobe	Provenance for the piece

Screen and tap trail	30 days	Diagnostics and product improvement
fields)		
Body figures for try-on	Until you delete them or your account is erased	Reuse without re-upload
Data export link	8 days	Your download
Partner Stylist access log	Life of the grant plus 3 years	Your record of who looked
Moderation decisions, reports, appeals	3 years	Transparency reporting; repeat-breach assessment; regulatory requests
In-person booking records and safety reports	7 years	Safety; legal claims
Criminal-history results (Stylists)	Result only, while the Stylist is active, then deleted; the report itself is not retained	Data minimisation
Consent and marketing preferences	While your account is open and for 3 years after (so we can honour your opt-out)	Evidence of consent (subscription consents: term plus 3 years)
Age-assurance evidence	Result only; evidence deleted within 30 days	Data minimisation
Analytics (Firebase, website)	26 months, or de-identified; website traffic beacon 180 days	Improvement
Crash and performance reports (MetricKit)	90 days	Diagnostics
Support and complaints	3 years from closure	Follow-up and legal claims
Legal claims and holds	Until the matter is closed	Establishing and defending claims
Security, sign-in and admin audit logs	12 months (sign-in); 3 years (administrative actions)	Security; breach investigation; accountability
Photographs you upload for virtual try-on	Deleted by us and by the image provider on completion of the try-on; not retained	Data minimisation
Record of privacy requests and our responses	3 years from closure	Accountability
Data breach register	5 years (Canada: at least 24 months)	Accountability

Where a period above is shorter than the law of your country requires, or longer than that law allows, the law's period applies.

9. Your rights

9.1 What you can ask for. Wherever you live, you can ask us to: tell you whether we hold personal information about you and give you access to it and a copy; correct it; delete it; give you a copy in a structured, machine-readable format (portability); restrict how we use it; object to a use based on legitimate interests, including profiling; opt out of direct marketing at any time; withdraw a consent at any time (without affecting what we did before); and have a person review a significant automated decision. Some countries give you further rights, listed in the Annexes.

9.2 How to ask. You can make a request at Settings > Privacy, by email to privacy@nupare.com.au, or by post. In Settings > Privacy you can request a download of your data (the link works for 8 days), delete your account (which takes effect after a 30-day grace period, during which you can change your mind) and manage your consents yourself. You can also ask through an authorised agent; we verify that the agent has your authority.

We do not charge for requests unless they are manifestly excessive, in which case we may charge a reasonable fee or decline and tell you why.

9.3 Verification. We verify that a request comes from you (or your agent) using information on your account and, where necessary, by asking you to confirm through your account email. We do not ask for more than we need.

9.4 Timing. We respond within one month in the EEA, UK and Switzerland (extendable by two further months for complex requests, with notice); 45 days in the United States (extendable by 45 days with notice); 30 days in Australia, Canada, Singapore and Japan; 20 working days in New Zealand; 40 days in Hong Kong; 10 days in Korea; 21 days in Malaysia; and, elsewhere, within the shorter of 30 days and the period the law of your country requires. If we need longer we tell you why.

9.5 Limits. We may refuse or limit a request, and may keep and use information, where the law allows or requires it: to comply with a legal obligation (tax, anti-money-laundering, marketplace-verification, product-safety, content-moderation and transparency-reporting records); to complete a transaction you have started or to administer a claim, return, chargeback or payout; to establish, exercise or defend a legal claim, including one that has not yet been brought where we reasonably expect it; to prevent, detect or investigate fraud, counterfeiting or misuse of the Service; to protect the safety of a person; to keep the record we need to honour your opt-out or deletion request; where granting the request would disclose another person's personal information or our confidential or legally privileged information; or where a request is manifestly unfounded or excessive. Where we refuse a request in whole or part, we tell you why and how to complain and appeal.

9.6 Human review of automated decisions. If an automated decision described in section 4.1 significantly affects you, you can ask at Settings > Help > Appeal a decision or by email for a person to review it, tell you the main factors, and let you make your case. We respond within 10 business days where practicable.

9.7 No discrimination. We do not treat you differently for exercising a privacy right, except that a feature that needs the information you have asked us to delete may no longer work.

10. Marketing and communications

10.1 Service messages. We send transactional and service messages (order confirmations, dispatch, payout notices, booking confirmations, Insider reminders, safety notices and changes to terms) to everyone with an account; these are not marketing and you cannot opt out of them while your account is open.

10.2 Marketing. We send marketing email, push notifications and SMS only where the law of your country allows. In most countries we ask for your consent first, using a separate, unselected option; in the UK and a few other countries we may email you about our own similar products after a purchase unless you opt out. Marketing SMS always requires your separate express consent. Push notifications are sent for the kinds of event you turn on at Settings > Notifications; marketing pushes are off until you turn them on. Every marketing message tells you how to unsubscribe, and we honour opt-outs within 5 business days (within 10 business days in the United States and Canada as the law allows, though our standard is 5). You can change every channel at Settings > Notifications.

10.3 Advertising on other platforms. We do not currently show NuPARE advertising to you on other platforms using your personal information, and we do not disclose identifiers or

hashed contact details to advertising networks or data brokers for that purpose. If we introduce it, we will update this Policy and the register in Annex N before it starts, ask for your consent where the law requires it, and make it controllable at Settings > Privacy > Advertising, through your device's advertising settings and, in the United States, through the "Your Privacy Choices" link and the Global Privacy Control signal, which we honour in any event.

10.4 Referrals. If a member refers you, we send one message that identifies the referring member, says why you are receiving it and how to have your details deleted; we send no further messages unless you join.

11. Cookies, SDKs and tracking

Annex N to this Policy (our Cookie and Tracking Policy, also published at nupare.com.au/legal/privacy#annex-n) lists every cookie, software development kit and similar technology we use on the website and in the app, who provides it, what it does, how long it lasts, and how to control it, and explains how consent works in your country. Strictly necessary technologies run without consent; everything else runs only with your consent where your country requires it, and you can change your choice at any time at Settings > Privacy > Cookies and tracking.

12. Children

The Service is for people aged 16 and over, or the higher minimum age set for your country in Schedule 1 to the Terms. We do not knowingly collect personal information from anyone under the minimum age. For members under 18 we set the most protective settings by default: private account, presence off, no advertising based on profiling, and no direct messages from members they do not follow. These defaults apply from the date stated on the Age Assurance Statement; before that date, you can set each of them yourself at Settings > Privacy. We do not use the information of members under 18 for targeted advertising, and we do not sell or share it. The protections of the Australian Children's Online Privacy Code, the UK Age Appropriate Design Code, Article 28 of the EU Digital Services Act and the US state minors' provisions apply. We use the age-assurance measures described in our Age Assurance Statement (Policy 8 in Schedule 6 to the Terms, published at nupare.com.au/legal/age-assurance), which states which measures are in operation in your country, and we keep only the result. If we learn that an account belongs to a person under the minimum age, we close it and delete the information. If you are a parent or guardian and you believe a child has an account, you may tell us at privacy@nupare.com.au. We do not profile for advertising, or serve advertising based on profiling, to anyone we know to be under 18.

13. Data breaches

Where we suspect an eligible data breach we complete an assessment within 30 days. Where we believe on reasonable grounds that a breach of security affecting your personal information is likely to result in **serious harm**, we notify the Information Commissioner and you as soon as practicable, unless remedial action removes that likelihood. We tell you without undue delay, explaining what happened, what information was involved, what we are doing and what you can do. We notify the privacy regulator where the law requires (for example within 72 hours in the EEA, the UK, Korea, Malaysia and Saudi Arabia; within 3 days

in Singapore; as soon as practicable in Australia, New Zealand and Canada; and within the periods the Annexes describe).

14. Changes to this Policy

We may update this Policy to reflect changes in the law, the Service or our practices. We tell you at least 30 days before a material change takes effect, by email and in the app, and we ask for your consent where a change would use your information for a new purpose that requires it. Every version and its effective date is at nupare.com.au/legal/privacy.

A change that does not affect your rights (correcting a typographical error, or adding a sub-processor of a kind already described) may be made without that notice and is recorded in the version history. Where a change does not require your consent, it takes effect on the date we state. This Policy is a notice about how we handle personal information and is not a contract, except where Schedule 1 to the Terms of Service says otherwise for your country: your continued use of the Service is therefore not your agreement to anything for which the law requires consent.

15. Complaints

If you have a concern about how we handle your personal information, contact our Privacy Officer at privacy@nupare.com.au or through Settings > Privacy > Make a complaint. We acknowledge every complaint within 2 business days, investigate it, and give you a written response within 30 days. If you are not satisfied, you can complain to the privacy regulator where you live; the Annexes name them. In the UK the Information Commissioner may decline to consider a complaint that has not first been raised with us.

16. Business contacts

If you work for a brand, retailer, media outlet, agency or other business with which we deal, we hold your business contact details (name, role, employer, work email and phone, and notes of our dealings) in our relationship system. We obtain them from you, from your employer, from public sources (company websites, professional networks) and from business-data providers. We use them to manage our commercial relationships and to contact you about NuPARE's services for brands, on the basis of our legitimate interests (and, where required, your consent). We keep them while the relationship or prospect is live and for 2 years after our last contact. Where the law requires us to tell you within a month that we obtained your details from a source other than you, we do so by email at first contact. You may object or ask us to delete them at any time at privacy@nupare.com.au. The rest of this Policy applies to you with the necessary changes.

17. Definitions

"Personal information" means information that relates to an identified or identifiable individual, including information from which an individual can be singled out, and includes "personal data" and equivalent terms in the laws of the countries in which we operate. Terms used in this Policy have the meaning given in the Terms of Service.

Regional Annexes

Each of Annexes A to M applies to you if you live in the country named, and adds to (and where inconsistent, overrides) sections 1 to 16. Annexes N to R follow them and also form part of this Policy.

Annex A: Australia

A.1 This Policy is our privacy policy for the purposes of Australian Privacy Principle 1 in the Privacy Act 1988 (Cth). We are bound by the Australian Privacy Principles wherever we operate.

A.2 Automated decisions. Section 4 sets out the kinds of personal information used by computer programs to make, or to do things substantially and directly related to making, decisions that could reasonably be expected to significantly affect your rights or interests; the kinds of decisions made entirely by those programs; and the kinds of decisions in which they substantially assist a person, as Australian Privacy Principle 1.7 will require from 10 December 2026.

A.3 Overseas disclosure. We disclose personal information to recipients in the United States, the European Union, the United Kingdom, Singapore and Japan (section 6.1) and to members and Providers in the countries where they are located. We take reasonable steps to ensure that overseas recipients handle your information in accordance with the Australian Privacy Principles, and we remain accountable for them under Australian Privacy Principle 8 unless an exception applies.

A.4 Anonymity. You can browse the Service without an account. You cannot transact anonymously because we must identify the parties to a sale or booking and comply with payment and verification laws.

A.5 Government identifiers. We do not use a government identifier (such as a passport or driver's licence number) as your account identifier.

A.6 Access, correction and complaints. Sections 9 and 15 explain how to access and correct your information and how to complain. You may also complain to the Office of the Australian Information Commissioner at oaic.gov.au.

A.7 Notifiable data breaches. We comply with the Notifiable Data Breaches scheme in Part IIIC of the Privacy Act.

A.8 Direct marketing. You can opt out of direct marketing at any time (Australian Privacy Principle 7) and, on request, we will tell you the source of the information we used.

A.9 Unsolicited information (Australian Privacy Principle 4). Where we receive personal information we did not ask for (including messages in a connected mailbox that turn out not to be receipts) and it is not information we could have collected under Australian Privacy Principle 3, we destroy or de-identify it as soon as practicable and lawful, and we do not index or retain it.

A.10 Correction (Australian Privacy Principle 13). Where we correct information we have already disclosed to someone else, we notify each recipient of the correction if you ask and it is practicable to do so. If we refuse to correct something, we tell you why and, if you ask,

we associate with the record a statement that you consider it inaccurate, out of date, incomplete, irrelevant or misleading.

A.11 Marketing, the Spam Act and the Do Not Call Register. Marketing email and SMS to Australian addresses and numbers comply with the Spam Act 2003 (Cth), including consent, accurate identification of us as sender and an unsubscribe facility we honour within 5 working days, and marketing calls comply with the Do Not Call Register Act 2006 (Cth). Notices about your account, an order, a booking, a decision or the end of an Insider term are service messages rather than marketing and are sent whatever your marketing preferences.

A.12 Collection notices (Australian Privacy Principle 5). We give the notice Australian Privacy Principle 5 requires at or before the point of collection: on the sign-up screen, in the in-app collection notice for each feature that collects something new, on the mailbox authorisation screen before you connect an account, on the consent screen for any face or body feature, and in the referral notice sent to a person you invite.

A.9 Online safety, the social media minimum age, and children. We may disclose information to the eSafety Commissioner and to law enforcement in accordance with the Online Safety Act 2021 (Cth). We have assessed the Service against the social media minimum age obligations in Part 4A of that Act and treat it as an age-restricted social media platform, because it offers a recommender feed, follows, comments, stories, direct messages and live broadcasts. The minimum age in Australia is accordingly 16, and we take the steps described in our Age Assurance Statement to prevent anyone under 16 from holding an account. We keep only the result of an age check, delete the evidence within 30 days, and do not use age-assurance information for any other purpose. We apply the Children's Online Privacy Code to members under 18.

Annex B: New Zealand

B.1 We are an agency carrying on business in New Zealand for the purposes of the Privacy Act 2020, and the Information Privacy Principles apply to us in relation to New Zealand users.

B.2 Collection notice. Section 2 states the purposes of collection, the intended recipients, our name and address, whether supply is voluntary or mandatory and the consequences of not supplying, and your rights of access and correction, as Information Privacy Principle 3 requires. Section 2.3 gives the notice required by Information Privacy Principle 3A when we collect information about you from someone else; where we rely on an exception to that Principle, we record why.

B.3 Cross-border disclosure. We disclose personal information to recipients outside New Zealand as section 6 describes. Where a recipient is not subject to privacy laws providing comparable safeguards to the New Zealand Act, we rely on binding contractual clauses or your authorisation given after we have expressly told you that the recipient may not be required to protect the information in a way that provides comparable safeguards (Information Privacy Principle 12).

B.4 Breaches. We notify the Privacy Commissioner and affected individuals of a notifiable privacy breach as soon as practicable.

B.5 Access and correction. We respond within 20 working days. You may complain to the Office of the Privacy Commissioner at privacy.org.nz.

Annex C: United Kingdom

C.1 Representative. Our UK representative under Article 27 of the UK GDPR is named, with a UK postal address, on the Legal Contacts page.

C.2 Legal bases. Section 3 sets out the legal bases on which we rely under Article 6 of the UK GDPR, including the specific legitimate interests. Where we rely on a "recognised legitimate interest" under the Data (Use and Access) Act 2025 (for example crime prevention or safeguarding), we say so in the assessment you can request.

C.3 Your rights. In addition to section 9, you have the right to lodge a complaint with the Information Commissioner's Office (ico.org.uk). We respond to requests within one month, which we may extend by two months for complex requests. Where we reasonably need more information to identify you or the information you want, the time is paused until you provide it. We conduct reasonable and proportionate searches.

C.4 Complaints procedure. In accordance with section 164A of the Data Protection Act 2018, you can complain to us through Settings > Privacy > Make a complaint or by email. We acknowledge your complaint within 30 days (our standard is 2 business days) and respond without undue delay.

C.5 Automated decisions. Where we make a decision based solely on automated processing that has legal or similarly significant effects for you, we tell you, and you can obtain human intervention, express your view and contest the decision, as Articles 22A to 22D of the UK GDPR require. We do not base such a decision on special-category data.

C.6 Marketing. We rely on the "soft opt-in" in regulation 22 of the Privacy and Electronic Communications Regulations 2003 to email you about our own similar products after you buy, with an opt-out at the time and in every message; all other marketing requires your consent.

C.7 Transfers. We make transfers from the UK to Australia and to other countries without adequacy regulations under the International Data Transfer Agreement or UK Addendum with a transfer risk assessment, and to US providers certified under the UK Extension to the Data Privacy Framework where applicable.

C.8 Children. We have assessed whether the Service is likely to be accessed by children for the purposes of the Age Appropriate Design Code and recorded our conclusion; section 12 applies.

C.9 Online safety. We process information to comply with our duties under the Online Safety Act 2023, including to conduct risk assessments, detect illegal content and respond to Ofcom.

Annex D: European Economic Area (and Switzerland)

D.1 Representative. Our representative in the Union under Article 27 of the GDPR is named, with a postal address in a Member State, on the Legal Contacts page. Our legal representative under Article 13 of the Digital Services Act is separately named there. For Switzerland, the Federal Act on Data Protection applies and our Swiss representative, where required, is named there.

D.2 Legal bases. Section 3 states the legal basis under Article 6(1) of the GDPR for each purpose, and the legitimate interests pursued where Article 6(1)(f) is relied on. Where processing is a legal obligation, the laws are named. Special categories of data are

processed only with your explicit consent (Article 9(2)(a)) or where necessary for legal claims.

D.3 Your rights. In addition to section 9, you have the right to lodge a complaint with the supervisory authority of the Member State where you live, work or where the alleged infringement occurred; a list is at edpb.europa.eu. You may object at any time to processing for direct marketing, and to processing based on legitimate interests on grounds relating to your particular situation.

D.4 Automated decisions. Some of the decisions in section 4.1 are made solely by automated means and may produce legal effects or similarly significantly affect you: in particular automated holds on a payout, automated blocking of a listing or payment, and automated removal of content matching known illegal material. Where we make such a decision we rely on Article 22(2)(a) (necessary for the performance of our contract with you) or Article 22(2)(b) (authorised by Union or Member State law to which we are subject, including anti-money-laundering, sanctions, product-safety and Digital Services Act obligations), and we apply the safeguards in section 9.6: we tell you that the decision was automated, and you can obtain human intervention, express your point of view and contest the decision. The logic involved is this: our systems score each transaction, listing, message or payout request against rules and models built from transaction history, device and usage signals, listing and message content and, for attribution, link data; a score above a threshold triggers the outcome described, and the significance and envisaged consequence is a temporary restriction on access to funds, on selling or on posting until a person has reviewed it. You can ask us for further detail at privacy@nupare.com.au. We do not base such decisions on special categories of personal data.

D.5 Digital Services Act. We process the information in clause 5.11 of the Terms about traders to comply with Article 30, publish trader information on listings under Article 30(7), notify affected consumers under Article 32, and keep records of notices, decisions and complaints under Articles 16, 17, 20 and 24. Information about your use of recommender systems is in clause 3.9 of the Terms.

D.6 Tax reporting (DAC7). If you sell or provide services through the Service and you are resident in a Member State, we are required by Council Directive (EU) 2021/514 to collect your name, address, date of birth, tax identification number, VAT number, financial account identifier and the consideration paid to you each quarter, and to report them annually by 31 January to the tax authority of the Member State in which we are registered, which exchanges them with the tax authority of your Member State. We tell you what we have reported. If you do not provide the information after two reminders and 60 days, we must suspend your account or withhold payment.

D.7 Product safety. We process purchase and contact information to comply with Regulation (EU) 2023/988, including to notify you of a recall.

D.8 Cookies. We use non-essential cookies and similar technologies only with your consent under the national laws implementing Article 5(3) of Directive 2002/58/EC. "Reject all" is as prominent as "Accept all". You can withdraw consent as easily as you gave it.

D.9 Transfers. Australia has no adequacy decision: we make transfers to us and to our Australian providers under the standard contractual clauses with a transfer impact assessment. We make transfers to the United States to providers certified under the EU-US Data Privacy Framework for the relevant data, with the standard contractual clauses as a

fallback, or under the clauses alone. You can obtain a copy of the clauses from privacy@nupare.com.au.

D.10 Germany. Our Datenschutzerklärung in German is at nupare.com.au/de/datenschutz. We send marketing email only with your consent under § 7 UWG, except for the narrow exception in § 7(3).

D.11 France. The French version of this Policy applies to you. We refresh cookie consent at least every 6 months.

D.12 Spain and the rest of the EEA. We refresh cookie consent at least every 24 months.

D.13 Criminal-offence data. We process data relating to criminal convictions about a Stylist in the EEA only where the law of the Member State expressly authorises a check for this activity and provides appropriate safeguards (Article 10 of the GDPR).

Annex E: United States

E.1 Scope. This Annex applies to residents of California, Colorado, Connecticut, Delaware, Florida, Indiana, Iowa, Kentucky, Maryland, Minnesota, Montana, Nebraska, New Hampshire, New Jersey, Oregon, Rhode Island, Tennessee, Texas, Utah, Virginia and any other state whose privacy law applies to us. Where a state's law gives you a right described here, it applies; where it does not, we honour the right anyway as a matter of policy.

E.2 Categories collected, sources, purposes and disclosures. In the 12 months before the date of this Policy we collected the following categories of personal information, from the sources in section 2, for the purposes in section 3, and disclosed them for a business purpose to the categories of recipients in section 5: identifiers (name, email, phone, address, username, IP address, device identifiers, account identifiers); customer records (billing and delivery address, payment method token, tax identification number and government identification for Sellers and Providers); characteristics of protected classifications (age; and, only if you enter them, measurements that may indicate pregnancy or disability); commercial information (purchases, sales, bookings, returns, Points, subscriptions); internet and network activity (usage, searches, interactions, cookie and SDK data); geolocation (approximate from IP; precise only with permission); audio or visual information (profile and listing photographs; a selfie if you choose that verification method); professional information (business details for Sellers and Providers); inferences (preferences used for personalisation); and sensitive personal information (government identification numbers and documents, financial account details collected by our payment provider, precise geolocation with permission, account login credentials, and, for Stylists, criminal-history results). We retain each category for the periods in section 8.

E.3 Sale and sharing. We do not sell personal information for money. We do not currently "share" personal information (as California defines it) or process it for "targeted advertising" (as other states define it). The only cross-context activity on the Service is Creator affiliate attribution, which uses a click token that does not identify you to the network. We nevertheless honour the Global Privacy Control and other universal opt-out signals recognised by your state, and we provide the "Your Privacy Choices" link on our website and Settings > Privacy > Advertising, so that your choice is recorded before any such processing could begin; if we ever introduce it, we update this Annex and section 10.3 first. We do not sell or share the personal information of anyone we know to be under 16, and we do not process the personal information of anyone we know to be under 18 for targeted advertising or sell it.

E.4 Sensitive personal information. We use sensitive personal information only to provide the Service you request, verify identity as the law requires, prevent fraud and protect safety, and comply with law. We do not use it to infer characteristics. In states other than California we obtain your consent before collecting it; in California you can limit its use at "Your Privacy Choices", though the uses above are those the law permits without limitation.

E.5 Your rights. You have the right to know what personal information we collect, use, disclose, sell or share; to access it and obtain a copy in a portable format; to correct it; to delete it; to opt out of sale, sharing, targeted advertising and profiling in furtherance of decisions that produce legal or similarly significant effects; to limit the use of sensitive personal information (California); and not to be discriminated against for exercising these rights. You may submit a request at Settings > Privacy, through the web form at nupare.com.au/legal/privacy-request, by email to privacy@nupare.com.au, or through an authorised agent. We respond within 45 days, extendable once by 45 days with notice. If we deny your request you may appeal by replying to our response or emailing privacy@nupare.com.au with "Appeal" in the subject; we respond to appeals within 45 days (60 in some states) and tell you how to contact your state Attorney General if you disagree.

E.6 Notice of financial incentive (NuPARE Points). NuPARE Points are a loyalty program in which you earn Points on what you spend and redeem them against purchases on the Service, at the earn and redemption rates published at Account > Rewards, currently 2.5 Points for every A\$100 of eligible spend, with 100 Points worth A\$10. To run it we collect and use your identifiers and commercial information (what you buy and when), and we use your activity to personalise Points offers. You opt in by making a purchase with an account; you can opt out at any time by emailing privacy@nupare.com.au or closing your account; if you do, you have 60 days to redeem your Points under clause 7.3 of the Terms (Quebec residents: Points expire only after 12 months' inactivity). We offer this incentive because the information lets us operate the program and understand purchasing; we have estimated the value of a member's information to us at approximately A\$4 per member per year, calculated as the incremental gross margin attributable to program members' additional purchases divided by the number of members, and we consider the incentive (0.25% of eligible spend returned as Points) reasonably related to that value. The program is available on the same terms to all members.

E.7 Automated decision-making technology. Section 4 describes our automated decision-making. Where California's regulations require it (from 1 January 2027 for decisions in scope), we give you a pre-use notice, the right to opt out of automated decision-making used for a significant decision, and, on request, information about the logic and how it affected you. Some of the automated decisions in section 4.1 (in particular automated holds on a Seller's, Provider's or Creator's payout, automated suspension of the ability to sell or provide services, and automated decisions on Creator eligibility and commission) may be "significant decisions" concerning compensation for an independent contracting opportunity under those regulations. From 1 January 2027 we will, for any such decision: give you a pre-use notice before we use the technology; offer you the right to opt out, except where we rely on the security, fraud-prevention and safety exception, in which case we tell you so and a person reviews the decision at your request; and, on request, give you the logic of the technology, its output about you and how it was used. You can exercise these rights at Settings > Privacy or by email to privacy@nupare.com.au. We conduct and keep current the risk assessment the regulations require for this processing and for our use of identity-verification technology.

E.8 Children and minors. The minimum age in the United States is 16. We do not knowingly collect personal information from children under 13 and we are not directed to them; if we learn we have, we delete it. We treat the personal information of members aged 16 and 17 as section 12 and E.3 describe.

E.9 California: additional matters. We provide at least two ways to make a request, a web form and email, and we do not use "dark patterns" in our consent or opt-out flows. We are not a data broker; our privacy settings default to the most protective setting, and precise geolocation is off by default. Under the California Delete Act we do not sell data to parties with whom you have no relationship. Under Civil Code section 1798.83 you may request a notice of disclosures to third parties for their direct marketing; we make none.

E.10 Washington, Nevada and Connecticut consumer health data. If we collect information that is "consumer health data" under the Washington My Health My Data Act or Nevada SB 370 (for example body measurements you enter for maternity or adaptive sizing), our Consumer Health Data Privacy Policy (linked separately from our homepage at nupare.com.au/legal/consumer-health-data and reproduced at the end of this Policy) applies, we collect it only with your separate consent, we do not share it without a further separate consent, and we do not sell it.

E.11 Biometric information. If you choose an identity-verification method that uses a facial scan, or opt in to a feature that uses a scan of your face or body, we give you a separate written notice of the purpose and retention period and obtain your written release before collection, as the Illinois Biometric Information Privacy Act, the Texas Capture or Use of Biometric Identifier Act and similar laws require. The template is deleted within 30 days of verification, or when the purpose is satisfied, and never later than 3 years after your last interaction. We do not sell, lease or trade it. Our retention and destruction schedule is in Annex R.

E.12 Seller information. The INFORM Consumers Act requires us to collect, verify and, for high-volume Sellers, publish the information in clause 5.11 of the Terms. Tax information, including taxpayer identification numbers, is disclosed to the Internal Revenue Service and state tax authorities as the law requires.

E.13 Disputes about this Policy. If you live in the United States, a dispute about this Policy or about our handling of your personal information is a dispute relating to the Service for the purposes of clauses E.19 to E.27 of Schedule 1 to the Terms of Service, and is resolved by binding individual arbitration unless you opted out under clause E.21 or those clauses exclude it. They do not apply to a request or appeal under E.5 of this Annex, which we handle as this Annex describes; to a complaint to your state Attorney General, to a state regulator or to the Federal Trade Commission; to a claim for public injunctive relief on behalf of the general public; or to any claim that the law of your state does not permit to be arbitrated. Nothing in this Annex or in those clauses waives or limits a right you have under California Civil Code section 1798.150 or any other right that section 1798.192 protects from waiver.

Annex F: Canada

F.1 Accountability. Our Privacy Officer (section 1.2) is accountable for our compliance with the Personal Information Protection and Electronic Documents Act and the substantially similar laws of Alberta, British Columbia and Quebec.

F.2 Consent. We collect, use and disclose personal information with your meaningful consent, which sections 2 and 3 are designed to inform, including the risk of harm described in section 6.3. We obtain express consent for sensitive information and for marketing. You may withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice; we tell you the consequences.

F.3 Processing outside Canada. Your personal information is stored in Australia and processed by our service providers in Australia, the United States, the European Union, the United Kingdom and Singapore, and may be accessed by the courts, law enforcement and national security authorities of those countries under their laws. We use contractual and other means to provide a comparable level of protection.

F.4 Access and complaints. We respond to access requests within 30 days. You may complain to the Office of the Privacy Commissioner of Canada (priv.gc.ca) or your provincial commissioner.

F.5 Breaches. We report breaches creating a real risk of significant harm to the Privacy Commissioner and affected individuals, and keep a record of every breach for 24 months.

F.6 Alberta. For questions about our service providers outside Canada, contact our Privacy Officer at privacy@nupare.com.au; written information about our policies and practices in that respect is available on request.

F.7 Quebec. Our Privacy Officer is the person in charge of the protection of personal information under section 3.1 of the Act respecting the protection of personal information in the private sector; their title and contact information are on the Legal Contacts page. At the time of collection we tell you the purposes, the means of collection, your rights of access and rectification, your right to withdraw consent, the names of third parties for whom the information is collected where applicable, and that the information may be communicated outside Quebec; a privacy impact assessment has been conducted for communications outside Quebec and the transfers are governed by written agreements (section 17 of that Act). Our technological products are set to the highest level of confidentiality by default (section 9.1 of that Act). Before using technology that allows you to be identified, located or profiled, we tell you that we are doing so and how to deactivate it (section 8.1 of that Act); non-essential cookies and tracking are used only with your consent, requested separately. If we make a decision about you based exclusively on automated processing, we tell you at the latest at the time of the decision and, on request, the personal information used, the reasons and principal factors and parameters, and your right to have it corrected, and you may submit observations to a person who can review the decision (section 12.1 of that Act). You have the rights of access, rectification, portability (a copy of computerised information collected from you, in a structured, commonly used technological format) and de-indexation, and to complain to the Commission d'accès à l'information. This Policy is available in French at nupare.com.au/fr-ca/confidentialite.

Annex G: Singapore

G.1 This Policy is our notification under section 20 of the Personal Data Protection Act 2012. Our Data Protection Officer's business contact information is privacy@nupare.com.au (section 1.2). We rely on the legitimate interests exception in Part 3 of the First Schedule for fraud prevention, security and the improvement uses in section 3, having conducted the assessment the Act requires; and on deemed consent by contractual necessity for disclosures to Sellers and Providers. We do not rely on deemed consent by notification for

marketing. We transfer personal data outside Singapore under contractual obligations that provide a comparable standard of protection (regulation 10 of the Personal Data Protection Regulations 2021). We notify the Personal Data Protection Commission of a notifiable data breach within 3 calendar days of assessing it. We respond to access and correction requests within 30 days. Marketing to a Singapore telephone number is sent only with clear and unambiguous consent or after checking the Do Not Call Registry. We do not collect or retain NRIC or FIN numbers or copies unless the law requires; our verification vendor returns a result only. You may complain to the Personal Data Protection Commission at pdpc.gov.sg.

Annex H: Japan

H.1 Published matters. For the purposes of Article 32 of the Act on the Protection of Personal Information: our name and address and the name of our representative are in section 1 and on the Legal Contacts page; the purposes of use of retained personal data are in section 3; the procedures and fees for disclosure, correction, suspension of use and deletion are in section 9 (no fee); our complaint contact is privacy@nupare.com.au; and our security control measures are in section 7, including that personal data is handled in Australia and the United States and that we have assessed the data protection systems of those countries.

H.2 Cross-border transfers. Before we transfer your personal data to a third party outside Japan on the basis of your consent, we tell you: the countries to which the data is transferred (Australia, the United States, the European Union, the United Kingdom and Singapore); information about each country's personal-data protection system (Australia's Privacy Act 1988 establishes principles-based protection enforced by the Office of the Australian Information Commissioner, with no general adequacy recognition by Japan; the United States has no comprehensive federal law, with sectoral and state laws and enforcement by the Federal Trade Commission and state authorities, and is not recognised as adequate by Japan; the European Union and the United Kingdom are recognised by the Personal Information Protection Commission as having equivalent systems under Article 28; Singapore's Personal Data Protection Act 2012 establishes consent-based protection enforced by the Personal Data Protection Commission, with no adequacy recognition by Japan); and the measures the recipient takes (contractual obligations equivalent to the Act's requirements, and the security measures in section 7). Transfers to our own systems in those countries are made under those same measures. A summary of each country's system is in Annex Q.

H.3 Personally referable information. Where we provide identifiers such as cookie or advertising IDs to a third party that will link them to you, we confirm that the third party has obtained your consent, as Article 31 requires.

H.4 Breaches. We report to the Personal Information Protection Commission and notify you of breaches within the scope of Article 26.

H.5 External transmission. We publish the information required by Article 27-12 of the Telecommunications Business Act about information transmitted from your device to third parties (the content, the recipient and the recipient's purpose) in Japanese at nupare.com.au/jp/gaibusoushin and in the app on first launch.

H.6 Marketing email. We send advertising email only with your prior opt-in consent, which we record, and every message identifies us and gives an opt-out.

H.7 Language. The Japanese version of this Policy applies to you.

Annex I: Hong Kong

I.1 Personal Information Collection Statement. This Annex, with sections 2, 3, 5 and 9, is our statement under Data Protection Principle 1(3) of the Personal Data (Privacy) Ordinance. Supplying your name, email, delivery address and payment details is obligatory to use the Service; if you do not supply them we cannot open your account or complete a transaction. Everything else is voluntary. Your data may be transferred to the classes of persons in section 5. You may send a request for access or correction to our Privacy Officer at privacy@nupare.com.au; we respond within 40 days. We show you a separate Personal Information Collection Statement, in Chinese and English, before we collect personal data at each collection point: when you create an account, when you create a listing, when you book a Provider, and when you complete verification.

I.2 Direct marketing. Before we first use your personal data (name, email, phone, purchase history and preferences) for direct marketing of NuPARE's services, Brand Partners' fashion items, Insider, Points offers and Provider services, we ask for your consent or indication of no objection through a separate channel, and you may opt out at any time free of charge. We do not provide your personal data to any other person for their direct marketing without your written consent.

I.3 Transfers. Section 33 of the Ordinance is not in force. We transfer personal data to Australia and the United States under contractual safeguards modelled on the Privacy Commissioner's recommended model clauses.

I.4 Doxxing. We remove content that discloses personal data without consent with intent to cause harm, and comply with cessation notices from the Privacy Commissioner.

I.5 This Annex is available in Chinese and both versions are authoritative. You may complain to the Office of the Privacy Commissioner for Personal Data at pcpd.org.hk.

Annex J: Republic of Korea

J.1 Mandatory items. For the purposes of Article 30 of the Personal Information Protection Act: the purposes of processing are in section 3; the items collected and retention periods are in sections 2 and 8; third-party provision is set out in the table in J.1A and in section 5; our entrustees (수탁자) and the work entrusted are listed in Annex P; your rights and how to exercise them are in section 9; our Chief Privacy Officer's name and contact are on the Legal Contacts page and are privacy@nupare.com.au; our destruction procedure is that data is deleted or anonymised at the end of the period in section 8 by secure deletion, and paper is shredded; our safety measures are in section 7; the operation of automated collection devices (cookies) and how to refuse them is in section J.5; and the criteria and procedure for automated decisions are in section 4.

J.1A Third-party provision (제 3 자 제공). We provide personal information to third parties as follows. Where the law requires your consent, we obtain it separately and tell you that you may refuse and what happens if you do.

Recipient (제공받는 자)	Purpose (제공 목적)	Items (제공 항목)	Retention (보유·이용 기간)
The Seller or Brand Partner of an item you buy	Fulfilment of your order	Name, delivery address, order details	Until fulfilment is complete, then as the recipient's own law

Recipient (제공받는 자)	Purpose (제공 목적)	Items (제공 항목)	Retention (보유·이용 기간)
			requires
The Stylist or Care Provider you book	Performance of the booking	Name, booking details, session address (in-person only), piece details	30 days after the booking, except records the Provider's law requires
A gathering Organiser	Admission to the gathering	Name, ticket details	Until the gathering ends
A buyer with a claim against you as a Seller or Provider	Disclosure required by Article 20-3 of the E-Commerce Act	Your name, address and telephone number	Until the claim is resolved
Tax authorities, courts, regulators and law enforcement	Compliance with a legal obligation or lawful request	The items the law requires	The period the law requires

J.2 Consent. We obtain your consent separately for each purpose, distinguishing mandatory from optional items, and tell you the consequences of refusal. We do not refuse service because you decline an optional item or an optional app permission.

J.3 Overseas transfer. We transfer personal information to Australia (our own systems, hosted in Amazon Web Services' Sydney region) and to the United States, the European Union, the United Kingdom and Singapore (our service providers, each named with its country in Annex P). For each transfer we tell you: the items transferred (the categories in section 2 relevant to the purpose); the country, the date (at the time of collection and continuously thereafter) and the method (encrypted network transfer); the recipient's name and contact (listed in Annex P); the recipient's purpose and retention period (as in sections 3 and 8); and that you may refuse the transfer and the consequence (we cannot provide the Service, which is operated from Australia). Where the transfer is necessary to perform the contract, we rely on Article 28-8(1)(3) and disclose these matters here.

J.4 Breaches. We notify you and the Personal Information Protection Commission within 72 hours of becoming aware of a breach.

J.5 Cookies and automated collection. We use cookies and app identifiers to keep you logged in, remember preferences, analyse use and, with consent, for advertising. You can refuse cookies in a browser through its privacy or cookie settings (for example Chrome: Settings > Privacy and security > Cookies); on iOS, at Settings > Privacy > Tracking and Settings > Apple Advertising; and on Android, at Settings > Google > Ads. Refusing cookies may limit some features.

J.6 Automated decisions. You have the right to refuse a decision made solely by automated processing that significantly affects your rights or obligations, and to request an explanation; section 4 sets out the criteria and section 9.6 the procedure.

J.7 Marketing. We send advertising by electronic transmission only with your prior express consent, re-confirmed every 2 years, with "(광고)" at the start; night-time advertising requires separate consent. We collect your location only while you are using a feature that needs it (the weather for outfit suggestions, and finding nearby Providers) and we do not store it. Where we do so in Korea, we obtain your separate consent under the Act on the Protection, Use, etc. of Location Information, Before that consent we present separate Location-Based Service Terms, distinct from this Policy and the Terms, and we tell you the recipient and the purpose. You may at any time ask us, at privacy@nupare.com.au, for a

record of when your location information was used and to whom it was provided. We make the filings that Act requires before we enable any location feature in Korea.

J.8 Domestic representative. If the thresholds in Article 39-11 apply to us, we designate a domestic representative and name them on the Legal Contacts page.

J.9 The Korean version of this Policy applies to you. You may complain to the Personal Information Protection Commission or the Privacy Call Centre (118).

Annex K: Malaysia

K.1 This Annex, with sections 2, 3, 5 and 9, is our written notice under section 7 of the Personal Data Protection Act 2010, given in Bahasa Malaysia and English. The personal data we process, its sources, the purposes, the classes of third parties, your rights of access and correction and how to contact us, the choices you have to limit processing, and whether supply is obligatory (see section 2.5) are set out there. Our Data Protection Officer is notified to the Personal Data Protection Commissioner and reachable at privacy@nupare.com.au. We transfer personal data outside Malaysia to Australia and the United States on the basis of your consent, contractual necessity and our documented due diligence that the recipient provides an adequate level of protection, in accordance with the Cross-Border Personal Data Transfer Guidelines. We notify the Commissioner of a breach within 72 hours and you within 7 days where significant harm is likely. You have a right to data portability. We keep Seller records for 3 years as the Consumer Protection (Electronic Trade Transactions) Regulations require. You may complain to the Personal Data Protection Commissioner.

Annex L: United Arab Emirates

L.1 This Annex is our privacy notice under Federal Decree-Law No. 45 of 2021 on the Protection of Personal Data. Section 3 sets out our legal bases (consent, contract, legal obligation and legitimate interests). You have the rights of access, portability, rectification, erasure, restriction, objection to direct marketing and to automated processing, and to complain to the UAE Data Office. We transfer personal data to Australia, the United States, the European Union, the United Kingdom and Singapore under contractual clauses providing appropriate safeguards and, where required, your consent. We notify the Data Office of breaches and, where there is a high risk, you. The Executive Regulations to the Decree-Law have not yet been issued; we will update this Annex when they are. Federal Decree-Law No. 14 of 2023 applies to our handling of your information as a consumer. This Annex is available in Arabic, and the Arabic version prevails before a UAE court.

Annex M: Kingdom of Saudi Arabia

M.1 This Annex is our privacy policy under Article 12 of the Personal Data Protection Law (Royal Decree M/19 of 1443H as amended) and is made available to you before we collect your personal data. The legal basis and purpose of each collection are in section 3; whether supply is mandatory or optional and the consequences of refusal are in section 2.5; our identity and contact details are in section 1; the entities to whom we disclose data and why are in section 5; and your rights (to be informed, to access, to obtain a copy, to rectification and to destruction) and how to exercise them are in section 9. We are registered on the National Register of Controllers maintained by the Saudi Data and Artificial Intelligence Authority because we transfer personal data outside the Kingdom. Transfers to Australia,

the United States, the European Union, the United Kingdom and Singapore are made under the standard contractual clauses approved by SDAIA, with a risk assessment. We retain personal data collected in an e-commerce transaction only for the period the nature of the transaction requires, and use it for another purpose only with your prior consent; marketing is sent only with your prior opt-in consent. We notify SDAIA within 72 hours of a breach and you where there is serious harm. This Annex is available in Arabic, and the Arabic version prevails.

Further Annexes

Annexes N to R apply to everyone. Annex N is our Cookie and Tracking Policy. Annexes O to R reproduce, as part of this Policy, the pages that particular laws require us to publish at their own addresses.

Annex N: Cookie and Tracking Policy

This Annex is our Cookie and Tracking Policy. It forms part of this Policy and is also published on its own page. Where the law of your country requires a separate cookie notice, this Annex is that notice.

N.1 What this Annex covers

This Annex explains the cookies, software development kits (SDKs), pixels, local storage, device identifiers and similar technologies (together, **tracking technologies**) that we use on nupare.com.au and in the NuPARE app for iOS and Android, who provides them, what they do, how long they last, and how you control them. It applies alongside the main body of this Policy. Where this Annex refers to "cookies" it includes every tracking technology, in the app as well as on the website.

N.2 The four categories

Strictly necessary. These are needed to run the Service: keeping you logged in, remembering your basket and checkout state, security and fraud prevention, load balancing, recording your cookie choices, and (on the website) the consent banner itself. They run without consent because the Service does not work without them. You can block them in your browser or device, but the Service will not function.

Functional. These remember choices you make, such as language, currency, size and display preferences, and the state of the app between sessions. In the EEA and Quebec these run only with your consent; in the UK they run unless you opt out, as the Privacy and Electronic Communications Regulations (as amended by the Data (Use and Access) Act 2025) allow, and we give you a simple means to do so.

Analytics and performance. These tell us how the Service is used, which screens and features are popular, where errors occur, and how fast pages load, so we can improve it. In the EEA, Quebec, Korea and Saudi Arabia these run only with your consent; in the UK, analytics used solely to improve the Service run unless you opt out; elsewhere they run with notice and an opt-out.

Advertising and attribution. These measure whether our advertising on other platforms led you to NuPARE, attribute purchases to Creator links, and, with your consent, show you NuPARE advertising on other platforms based on your activity. They run only with your consent everywhere consent is required, and in the United States you can opt out under your state's law, including through the Global Privacy Control, which we honour. The app does not use Apple's App Tracking Transparency framework because it does not track you across other companies' apps and websites.

N.3 The register

The register below lists each tracking technology in use on the effective date of this Policy, on the website (nupare.com.au) and in the app. The live register, updated whenever a technology is added or removed, is at nupare.com.au/legal/privacy#register and in the app at Settings > Privacy > Cookies and tracking, and forms part of this Annex. "First party" means operated by us; "third party" means operated by the provider named.

App (iOS)

Name	Provider	Party	Category	Purpose	Duration
Session and device registry	NuPARE	First	Strictly necessary	Keeps you signed in (passkeys, two-step, Sign in with Apple or Google); registers your device for notifications and security alerts	While signed in; device entry until you sign out or delete the account
Screen and tap trail	NuPARE	First	Analytics and performance	Records the screens you visit and the controls you tap, batched about every 30 seconds, so we can reproduce problems and see how features are used	30 days
Firebase Analytics	Google	Third	Analytics and performance	Counts screens viewed and features used (pseudonymous app-instance identifier); no advertising use	26 months; app-instance identifier until reset
MetricKit reports	Apple (collected by NuPARE)	First	Analytics and performance	Crash and performance diagnostics	90 days
Google on-device conversion SDK	Google	Third	Advertising and attribution	Linked into the app by the Firebase framework but never called; no data is sent	Not used
Creator and affiliate click tokens	Awin, Rakuten Advertising, Commission Factory, Impact	Third	Advertising and attribution	When you follow a Creator's affiliate link, the network records the click so a later purchase can be attributed; the token does not identify you to the network	Up to 30 days, per network

The app declares no tracking under Apple's App Tracking Transparency framework: it does not link your data with third-party data for advertising and does not ask for the tracking permission. The app does not include Crashlytics; crash reports come to us through MetricKit.

Website (nupare.com.au)

Name	Provider	Party	Category	Purpose	Duration
Session and consent	NuPARE	First	Strictly necessary	Keeps you signed in on the web and records your cookie choices	Session; consent 6 months (France), 24 months (elsewhere)
np_vid, np_sid (localStorage)	NuPARE	First	Analytics and performance	A visitor identifier and session identifier for our own traffic measurement (/api/track), with	np_vid until cleared; np_sid for the session; traffic

Name	Provider	Party	Category	Purpose	Duration
)			ce	the page, referrer, city and country, browser type and campaign (UTM) parameters	records 180 days
nuPAREReferal (localStorage)	NuPARE	First	Functional	Remembers the member who referred you so they receive their Points when you join	30 days
Waitlist name and email (localStorage)	NuPARE	First	Functional	Remembers what you typed into the waitlist form	Until cleared
Google Analytics 4 (G-SZTQX191VZ)	Google	Third	Analytics and performance	Measures visits, pages and campaigns; advertising storage is denied and no advertising signals are sent	Up to 26 months
Stripe	Stripe	Third	Strictly necessary	Fraud prevention and payment on checkout and Insider pages	Session and up to 12 months
Support assistant	NuPARE	First	Functional	Keeps your support conversation open; the assistant answers from a written knowledge base and is not a generative AI model	Session

N.4 How consent works where you live

What runs today. In Australia and other countries whose law permits it, analytics technologies run with notice and an opt-out: Firebase Analytics is on by default and can be turned off at Settings > Privacy > Analytics; the screen and tap trail runs whenever you use the app and is deleted after 30 days and erased with your account; website analytics run by default and can be turned off at the "Cookie settings" link. Advertising and attribution technologies run only when you follow a Creator's affiliate link, and we run no advertising audience or conversion measurement. In countries whose law requires prior consent (the EEA, the UK for advertising technologies, Quebec, Korea, Saudi Arabia and others listed below), nothing beyond strictly necessary technologies runs until you agree; the settings below describe how we apply that by country. On the website we determine which configuration applies from the country your connection appears to come from, before any non-essential technology is set or read, using consent-mode regional defaults set to "denied" for the EEA, the United Kingdom, Switzerland and Quebec; in the app we use the country of your account and, before you have one, your app-store storefront. If we cannot determine your country, we apply the strictest configuration and nothing beyond strictly necessary technologies runs until you choose. The consent mechanisms described for each country below are in operation from the effective date of this Annex; the register at nupare.com.au/legal/privacy#register records the date each country's configuration went live.

EEA and Switzerland. On first use we show a banner with "Accept all", "Reject all" and "Manage choices" given equal prominence. Nothing other than strictly necessary technologies runs until you choose. Scrolling, continuing to browse or closing the banner is not consent. You can change or withdraw your choice at any time, as easily as you gave it, at Settings > Privacy > Cookies and tracking or the "Cookie settings" link in the website footer. We ask again after 6 months (France) or 24 months (rest of the EEA), or when we

add a technology in a category you have not consented to. We do not offer a "consent or pay" choice.

United Kingdom. Strictly necessary and functional technologies run with a clear notice. Our own screen and tap trail and our app analytics run on an opt-out basis, as the Privacy and Electronic Communications Regulations, as amended by the Data (Use and Access) Act 2025, allow for statistics used solely to improve the service. You can switch each of them off at any time at Settings > Privacy > Analytics and Settings > Privacy > Screen and tap trail, and we tell you so when you first open the app. We rely on that exemption for Firebase Analytics only on the basis that our contract with Google prohibits Google from using the data for its own purposes; if that ceases to be the case we will move Firebase Analytics to consent in the United Kingdom. Website analytics and all advertising and attribution technologies run only with your consent. The banner offers "Accept", "Reject" and "Manage choices" with equal prominence.

Quebec. Before any technology that can identify, locate or profile you runs, we tell you and how to deactivate it, and we obtain your consent, requested separately, for anything beyond strictly necessary. "Refuse all" is as prominent as "Accept all". The banner is in French.

Rest of Canada. We show a layered notice at first use and an easy, immediate opt-out for advertising and analytics. Advertising based on your activity is never a condition of using the Service and is not used for anyone we know to be under 18.

United States. We show a notice at collection. Advertising and attribution technologies that involve "selling" or "sharing" personal information, or "targeted advertising", can be turned off at the "Your Privacy Choices" link and at Settings > Privacy > Advertising, and we honour the Global Privacy Control and other opt-out preference signals recognised by your state's law. Residents of states that require it can opt in rather than out; where the law requires opt-in, we ask.

Australia and New Zealand. We show a notice at first use; analytics run by default and can be turned off (the screen and tap trail can be turned off at Settings > Privacy > Screen and tap trail, is deleted after 30 days in any event, and is erased with your account). We run no advertising technologies that single you out.

Japan. Before any information is transmitted from your device to a third party, we show (on first launch and on the website) the information required by Article 27-12 of the Telecommunications Business Act: what is transmitted, to whom, and for what purpose, in plain Japanese, with a toggle to turn off each non-essential technology. Where a third party will link an identifier to you, we confirm your consent as the Act on the Protection of Personal Information requires.

Korea. This Policy states how automated collection devices operate and how to refuse them (Annex J.5). We separate app permissions into mandatory and optional. Advertising technologies run only with your separate consent.

Singapore, Hong Kong and Malaysia. We show a notice at first use with a categorised table and an opt-out for analytics and advertising; advertising identifiers are treated as personal data and used for behavioural advertising only with your consent.

UAE and Saudi Arabia. Non-essential technologies run only with your consent, and the notice is in Arabic and English.

N.5 How to control tracking

In the app. Settings > Privacy > Analytics turns Firebase Analytics off; Settings > Privacy > Screen and tap trail turns the trail off; Settings > Privacy > Cookies and tracking shows every category and, in countries where consent applies, lets you change it. Deleting your account erases the trail, analytics identifiers and device registry.

On the website. The "Cookie settings" link in the footer reopens your choices. Your browser's privacy settings let you block or delete cookies; blocking strictly necessary cookies will stop the Service working. Sending a Global Privacy Control signal from your browser opts you out of sale, sharing and targeted advertising where your state's law recognises it, and we treat it as an objection to advertising technologies everywhere.

Affiliate links. When you follow a Creator's affiliate link, the network named on the link records the click; the Creator Standards (Policy 6 in Schedule 6 to the Terms) explain how commission is attributed.

Email. Our marketing emails contain a pixel that tells us whether the email was opened. You can block it by turning off image loading in your email client, and you can stop marketing email altogether at Settings > Notifications or the unsubscribe link in every message.

N.6 Do Not Track

We honour the Global Privacy Control signal as described above. We do not currently respond to the older "Do Not Track" browser setting, for which there is no agreed standard.

N.7 Changes

We update this Annex and the register whenever we add or remove a tracking technology. Material changes are notified in the app and, where a new technology needs your consent, we ask for it before it runs.

Annex O: Sub-processors

This Annex lists our principal sub-processors. It forms part of this Policy and is also published, and kept current between versions of this Policy, at nupare.com.au/legal/subprocessors (**the live page**).

Provider	Service	Processing location	Transfer mechanism (where required)
Amazon Web Services (Lambda, DynamoDB, S3, SES, Cognito, IVS, Bedrock, Titan)	Hosting, storage, email sending, sign-in, live video, AI inference	Australia (Sydney, ap-southeast-2); Bedrock via Australian and Asia-Pacific inference profiles; try-on replica cache in the United States (Oregon, us-west-2)	SCCs / IDTA / DPF (AWS certified)
Anthropic (Claude, via Amazon Bedrock)	AI text and extraction models	Australia and Asia-Pacific (Bedrock regions)	Bedrock terms; no training on inputs
Stability AI	Image generation for virtual try-on	United States (Oregon)	SCCs / DPF where certified
OpenAI	Image editing for virtual try-on	United States	SCCs / DPF where certified

Provider	Service	Processing location	Transfer mechanism (where required)
Google (Gemini API; Firebase Analytics; Google Analytics 4; Gmail API; Sign in with Google)	Piece drawings; app and website analytics; connected-mailbox reading; sign-in	United States and global	DPF (Google LLC certified) / SCCs
Microsoft (Graph, Teams, Entra)	Connected-mailbox reading; Stylist session invitations; brand SSO	United States / EU / Australia	DPF (certified) / SCCs
Apple (APNs; Sign in with Apple; speech recognition)	Push notifications; sign-in; on-device voice search	United States / on device	DPF / SCCs
Stripe	Payments, connected accounts, disputes, Insider billing	United States / Australia / EU	DPF (certified) / SCCs
Australia Post; AfterShip	Delivery tracking	Australia; AfterShip United States/Singapore	Contractual / SCCs
Awin; Rakuten Advertising; Commission Factory; Impact	Affiliate click and sale attribution (click tokens only)	EU/UK; United States; Australia; United States	No personal information transferred
Brave Software	Search grounding for AI answers (query text only)	United States	Contractual
Meta (Instagram, Facebook); TikTok; LinkedIn	Admin social connections and landing-page post sync (Brand Partner and NuPARE accounts only)	United States / global	Platform terms
Canva	Admin design tooling	Australia	Contractual
Support platform and email delivery providers	Support tickets; transactional and marketing email	Named on the live page	SCCs / DPF
Identity and age verification vendor (named on the live page before launch)	Identity-document checking; facial matching where you choose it; age estimation; sanctions and PEP screening, returning a result and document type only, and holding any document or template no longer than 30 days	Named on the live page	SCCs / IDTA / DPF where certified; contractual ban on retention beyond 30 days, on template reuse and on any use for the vendor's own purposes
Criminal-history check provider (named on the live page; Stylists only, where lawful)	Criminal-history check, result only	Country of the Stylist	Contractual; FCRA-compliant in the United States
Content moderation tooling provider (named on the live page)	Automated screening of listings, images, messages and reviews	Named on the live page	SCCs / DPF where certified
Business-contact data provider (named on the live page)	Enrichment of business contact records (section 16 of this Policy); no member personal information	Named on the live page	SCCs / DPF where certified

Changes to this Annex are announced 30 days in advance on the live page and by email to business users, who may object.

Annex P, Korea: 개인정보 처리위탁 및 국외이전 현황

(nupare.com.au/kr/entrustment · nupare.com.au/kr/transfer)

처리위탁 현황 (개인정보 보호법 제 26 조, 제 30 조). 당사는 서비스 제공을 위하여 아래와 같이 개인정보 처리업무를 위탁하고 있으며, 수탁자가 개인정보를 안전하게 처리하도록 관리·감독합니다.

수탁자	위탁업무	위탁 항목	보유·이용 기간
Amazon Web Services, Inc.	호스팅, 저장, 이메일 발송, 로그인, 라이브 영상, AI 추론	서비스 제공에 필요한 회원정보 일체	위탁계약 종료 또는 회원 탈퇴 시까지
Anthropic, PBC (Amazon Bedrock 경유)	AI 텍스트·추출 모델	입력 텍스트, 영수증·이메일 추출 항목	처리 즉시 삭제(학습 불가)
Stability AI Ltd; OpenAI, L.L.C.; Google LLC (Gemini)	가상 착용 이미지 생성, 의류 도안	착용용 사진, 의류 이미지	생성 완료 즉시 삭제
Google LLC (Firebase Analytics, Google Analytics 4)	앱·웹 이용 분석	가명처리된 인스턴스 ID, 이용 이벤트, 기기정보	26 개월
Stripe, Inc.	결제 처리, 정산, 분쟁 처리	결제정보, 계좌정보, 본인확인 결과	관련 법령상 보존기간
Microsoft Corporation	연결된 메일함 읽기, 스타일 리스트 세션 초대, 브랜드 SSO	이메일, 일정, 계정정보	연결 해제 시까지
Apple Inc.	푸시 알림, 로그인	기기 토큰, 계정 식별자	회원 탈퇴 시까지
AfterShip Limited; Australia Post	배송 추적	운송장 번호, 배송지	배송 완료 후 90 일
본인확인·연령확인 사업자 (Legal Contacts 페이지에 게시)	신분증 확인, 안면 대조(선택시), 연령 추정, 제재 대상 조회	신분증 이미지, 얼굴 이미지, 성명, 생년월일	30 일 이내 삭제(결과만 보관)
고객지원 및 이메일 발송 사업자 (nupare.com.au/legal/subprocessors 에 게시)	문의 처리, 거래·마케팅 이메일 발송	성명, 이메일, 문의 내용	처리 종료 후 3 년

국외이전 현황 (개인정보 보호법 제 28 조의 8). 당사는 호주 법인으로 회원의 개인정보를 아래와 같이 국외로 이전합니다. 이전을 원하지 않는 경우 계정 생성을 거부할 수 있으나, 이 경우 서비스(호주에서 운영)를 이용할 수 없습니다. 계약 이행에 필요한 이전은 제 28 조의 8 제 1항 제 3 호에 따라 본 페이지에 고지합니다.

이전받는 자(연락처)	이전 국가	이전 항목	이전 일시·방법	이용 목적	보유·이용 기간
Nu Pare Pty Ltd (privacy@nupare.com.au), AWS 시드니 리전	호주	개인정보 처리방침 제 2 조의 항목	수집 시점 및 이후 상시, 암호화된 네트워크 전송	서비스 제공	처리방침 제 8 조의 기간
Stripe, Inc. (privacy@stripe.com)	미국, 호주, EU	결제·계좌·본인확인 정보	결제 시, 암호화 전송	결제 처리	법령상 보존기간
Stability AI Ltd; OpenAI, L.L.C.	미국	가상 착용용 사진	기능 이용 시, 암호화 전송	이미지 생성	생성 즉시 삭제
Google LLC (privacy@google.com)	미국	분석 이벤트, 기기 정보, 연결 메일함	이용 시 상시, 암호화 전송	분석, 메일함 읽기, 로그인	26 개월 / 연결 해제 시까지

이전받는 자(연락처)	이전 국가	이전 항목	이전 일시·방법	이용 목적	보유·이용 기간
		데이터(선택 시)			지
Microsoft Corporation	미국, EU, 호주	연결 메일함 데이터, 일정, 계정정보	연결 시 상시, 암호화 전송	메일함 읽기, 세션 초대, SSO	연결 해제 시 까지
AfterShip Limited	싱가포르, 미국	운송장 번호, 배송지	발송 시, 암호화 전송	배송 추적	배송 완료 후 90 일
Awin Ltd; Rakuten Advertising; Impact Tech, Inc.	영국, EU, 미국	클릭 토큰(개인 식별 불가)	제휴 링크 클릭 시	성과 측정	90 일
본인확인 사업자 (Legal Contacts 페이지에 게시)	게시된 국가	신분증·얼굴 이미지, 성명, 생년월일	확인 시, 암호화 전송	본인·연령 확인	30 일 이내 삭제

이전 거부 및 문의: privacy@nupare.com.au. 본 현황은 변경 시 즉시 갱신하며, 개인정보 처리방침 부록 J에서 링크합니다.

Annex Q, Japan: 外国における個人情報の保護に関する制度 (nupare.com.au/jp/kaigai)

個人情報保護法第 28 条第 2 項および規則第 17 条に基づき、当社が個人データを提供する外国の制度について、個人情報保護委員会の公表資料を参照して以下のとおりお知らせします。当社は、いずれの提供先についても、提供先が講ずる措置（契約による同法相当の義務、当社プライバシーポリシー第 7 条の安全管理措置）を確認しています。

国・地域	個人情報の保護に関する制度の有無	主な法令および執行機関	事業者の義務・本人の権利に関する主な相違点	越境データ移転に関する制限
オーストラリア (当社自身のシステム、AWS シドニー)	あり (OECD プライバシーガイドラインに対応する制度あり。日本の十分性認定の対象外)	Privacy Act 1988 (豪州プライバシー原則)、Office of the Australian Information Commissioner	原則ベースの規律。本人の開示・訂正請求権あり。漏えい等の報告義務あり。2026 年 12 月 10 日以降、自動化された意思決定に関する開示義務あり	海外開示にあたり合理的措置を講ずる義務 (APP 8)
米国 (Stripe、Stability AI、OpenAI、Google、Microsoft、Apple、Brave)	連邦レベルの包括的制度なし。州法 (カリフォルニア州等) および分野別法令あり。日本の十分性認定の対象外	Federal Trade Commission Act §5、各州プライバシー法 (CCPA 等)、Illinois BIPA 等; FTC および各州司法長官	事業者の義務・本人の権利は州により異なる。政府機関による情報収集に関する法令 (FISA 702 等) が存在する	一般的な越境移転制限なし。EU-U.S. Data Privacy Framework による認証制度あり
欧州連合 (Stripe、Microsoft、Awin)	あり (日本と相互に十分性認定)	一般データ保護規則 (GDPR)、各加盟国の監督機関	日本法と同等以上の保護。本人の権利 (アクセス、消去、	十分性認定国以外への移転には標準契約条項等が必要

国・地域	個人情報の保護に関する制度の有無	主な法令および執行機関	事業者の義務・本人の権利に関する主な相違点	越境データ移転に関する制限
			可搬性、異議）が広い	
英国（Awin）	あり（日本と相互に十分性認定）	UK GDPR、Data Protection Act 2018、Data (Use and Access) Act 2025、Information Commissioner's Office	EU と同等の枠組み	十分性認定国以外への移転には IDTA 等が必要
シンガポール（AfterShip）	あり（日本の十分性認定の対象外）	Personal Data Protection Act 2012、Personal Data Protection Commission	同意を基本とする規律。本人のアクセス・訂正請求権あり。漏えい通知義務あり	移転先が同等の保護を提供することを確保する義務（Transfer Limitation Obligation）

各提供先の名称、所在国および連絡先は nupare.com.au/legal/subprocessors に掲載しています。本ページは制度の変更に応じて更新します。お問い合わせ: privacy@nupare.com.au

Annex R: Biometric Data Retention and Destruction Policy (United States), nupare.com.au/legal/biometrics

This Annex is our Biometric Data Retention and Destruction Policy. It forms part of this Policy, is also published on its own page at nupare.com.au/legal/biometrics, and is given under the Illinois Biometric Information Privacy Act (740 ILCS 14/15(a)), the Texas Capture or Use of Biometric Identifier Act, Washington's biometric identifier law (RCW 19.375) and Colorado's biometric provisions (C.R.S. 6-1-1314), and applies to every resident of a state whose law treats a scan of face or body geometry as a biometric identifier regardless of the purpose of collection.

What we collect and why. We may process an image that a state law treats as a biometric identifier in two situations only: (1) a photograph you choose to upload for virtual try-on, which we use solely to generate an image of you wearing a piece; and (2) a facial image you choose to submit for identity matching during Seller, Provider or age verification, which our identity-verification vendor compares with your identity document. We do not use either image to identify you in other content, to build a face or body template for recognition, to track you, or for any purpose other than the one you chose.

Notice and release. Before we process such an image we tell you in writing, on the screen where you upload it, that a biometric identifier may be collected, the specific purpose, and the length of time for which it is retained, and we obtain your written release, recorded with a timestamp. You may decline; the feature is then unavailable and nothing else about your account changes.

Retention and destruction schedule. We destroy a try-on photograph and any geometry derived from it when the try-on image has been generated, and in any event within 24 hours; we keep the generated image (which is not a biometric identifier) in your wardrobe

until you delete it. A facial image submitted for identity matching, and any template derived from it, is destroyed by our vendor within 30 days of the verification result and is never transmitted to us. In every case, destruction occurs no later than the earlier of the date on which the purpose for collection has been satisfied and 3 years after your last interaction with us. Destruction means permanent deletion from active systems and, for backups, expiry under our standard backup rotation within 35 days.

No sale, lease or profit; disclosure. We do not sell, lease, trade or otherwise profit from your biometric identifiers or biometric information. We disclose them only to the vendor performing the function you chose, under a contract that prohibits any other use, or where required by law or a valid warrant or subpoena.

Security. Biometric identifiers are stored and transmitted using at least the standard of care in our industry and in a manner at least as protective as that used for other confidential and sensitive information, including encryption in transit and at rest and access limited to the systems performing the function.

Contact. privacy@nupare.com.au; postal address on the Legal Contacts page. This Annex is reviewed annually and whenever a listed process changes.

Separately published notice

The following notice is published as a standalone page at nupare.com.au/legal/consumer-health-data, with its own link in the footer of our homepage, because the laws under which it is given require that it not be combined with this Policy. It is reproduced here for completeness.

Consumer Health Data Privacy Policy (Washington, Nevada, Connecticut): nupare.com.au/legal/consumer-health-data

This policy is published under the Washington My Health My Data Act (RCW 19.373), Nevada SB 370 and the consumer health data provisions of the Connecticut Data Privacy Act. It is linked from the footer of our homepage and is separate from our Privacy Policy, as those laws require.

Categories of consumer health data we collect. NuPARE is a fashion platform and does not offer health services. The only information we hold that may be "consumer health data" is information you choose to give us that reveals a physical characteristic for the purpose of fit: body measurements and body figures you create for sizing and virtual try-on, and the maternity or adaptive-sizing preferences you may select. We do not collect, infer or derive information about health conditions, treatments, reproductive or sexual health, gender-affirming care, or biometric data for health purposes, and we do not use geofencing around any health-care facility.

Sources and purposes. We collect this information only from you, only when you enter it, and only to recommend sizes, generate try-on images and filter listings by fit. We do not use it for advertising, profiling or ranking, and we do not share it for any purpose.

Sharing. We share body figures and measurements only with the processors that generate your try-on image (named on our sub-processor page at nupare.com.au/legal/subprocessors), under contracts that prohibit any other use, and with a

Stylist only where you have granted that Stylist access to your wardrobe and only for the duration of the grant. We do not sell consumer health data and will not do so without the separate, signed authorisation those laws require.

Your rights. You may confirm whether we collect or share consumer health data about you, access it, obtain a list of the third parties and affiliates with whom we have shared it, withdraw consent, and have it deleted, by emailing privacy@nupare.com.au or at Settings › Privacy. We respond within 45 days (extendable once by 45 days where reasonably necessary, with notice). If we deny a request, you may appeal by replying to our response; we decide the appeal within 45 days and tell you how to contact the Attorney General of your state if you are not satisfied. We do not discriminate against you for exercising these rights.

Retention. We keep body figures and measurements until you delete them or your account is erased, and they are deleted from our processors' systems when each try-on is complete.

Contact. privacy@nupare.com.au; postal address on the Legal Contacts page.

NuPARE Privacy Policy v2.0. © Nu Pare Pty Ltd 2026.