

360 Private Travel

Global Privacy Policy

Version 2.1. Effective date: 02 October 2026. This version replaces the Data Protection Privacy Policy dated 28 August 2026.

Part A. How we handle your personal data wherever you deal with us

1. Who we are and what this policy covers

360 Private Travel is a group of luxury travel companies operating from offices worldwide, as listed in the table in section 2. In this policy, **we, us, our** and **360 Private Travel** mean the group company that is responsible for your personal data, as explained in section 2.

This policy explains what personal data we collect about you, why we collect it, how we use, share and protect it, how long we keep it, and the rights you have. Part A applies to everyone we deal with, wherever you are. Part B adds information that applies in each of the countries where we have an office, because local law gives you additional rights or requires us to tell you additional things.

When we refer to **you**, we mean anyone whose personal data we process, including: the lead passenger or member; anyone else we communicate with about an enquiry, quote, membership or booking (for example the person who pays for the trip, a family office, an executive assistant or a corporate travel arranger); every person who travels or is intended to travel; the parents or guardians of any minors who travel; visitors to our websites and users of our member portal; and contacts at our suppliers and business partners.

Our websites include 360privatetravel.com and the 360 Juno member portal at 360juno.360privatetravel.com. Where a website or portal has its own specific notice, that notice supplements this policy.

2. Which 360 Private Travel company is responsible for your data

Each of the companies listed below is a data controller (the company that decides how and why your personal data is used) in its own right. The company responsible for your personal data is:

- for a booking or membership, the company named in your booking confirmation, membership agreement or invoice;
- for an enquiry or quote that has not yet become a booking, the company whose office or travel designer you are dealing with;
- for our websites, our marketing and our business contacts, 360 Private Travel Limited (United Kingdom), which operates our group websites and central systems, together with the group company for your region where one is involved.

Our group companies share central systems and support one another, for example when a travel designer in one office arranges travel that is fulfilled or supported by colleagues in another office, or when you travel through a region where we have a local team. Where two group companies decide together how your data is used, they act as joint controllers and have an intra-group data protection agreement in place that sets out their respective responsibilities. Whichever company is responsible, you can exercise your rights through the single contact point in section 21 and we will make sure your request reaches the right company.

Country	Company	Registered address	Registration and licences
United Kingdom	360 Private Travel Limited	54 High Street, Sevenoaks, Kent TN13 1JG, United Kingdom	Companies House 08512928; VAT 163818688; ATOL 7514; IATA 91200056
Australia	360 Private Travel Pty Ltd	Level 5, 179 Elizabeth Street, Sydney NSW 2000, Australia	ABN 93 685 913 071; IATA 96189833
Hong Kong	360 Private Travel Limited	Units 1001-03, 10/F, Prosperity Millennia Plaza, 663 King's Road, Quarry Bay, Hong Kong	BR 71239999-000-10-20-A; TIA licence 354498; IATA 13336153

Country	Company	Registered address	Registration and licences
Japan	360 Private Travel K.K.	8F Shinkawa Ohara Building, 1-27-8 Shinkawa, Chuo-ku, Tokyo 104-0033, Japan	Corporate number 0100-01-244642; IATA 96165845
Netherlands	360 Private Travel B.V.	Spaces Westerpark, Haarlemmerweg 331, 1051 LH Amsterdam, Netherlands	KvK 76863492; VAT NL860814579B01; ANVR 5749; IATA 96116370
Singapore	360 Private Travel Pte. Ltd.	22 Malacca Street, #03-02, RB Capital Building, Singapore 048980	UEN 202003026H; STB licence TA03387; IATA 96090492
Switzerland	360 Private Travel AG	Bellerivestrasse 203, 8008 Zürich, Switzerland	CHE-210.327.509; IATA 96097610
United Arab Emirates	360 Private Travel L.L.C-FZ	Meydan Grandstand, 6th Floor, Meydan Road, Nad Al Sheba, Dubai, United Arab Emirates	Licence 2533992.01; IATA 96210483
United States	360 Private Travel LLC	1688 Meridian Avenue, Suite 700, Miami Beach, FL 33139, United States	Registration Delaware LLC, file no. 5838999; Florida Seller of Travel ST 700358; IATA 08740664

3. Some words we use

Personal data (also called personal information in some countries) means any information relating to an identified or identifiable individual, such as your name, contact details, passport number, travel history or images of you.

Processing means anything we do with personal data, including collecting, recording, storing, using, analysing, sharing, transferring and deleting it.

Special category data or **sensitive data** means personal data that the law gives extra protection, for example information about your health, disability or mobility, dietary requirements that reveal a religious belief or health condition, racial or ethnic origin, biometric data, and, in some countries, passport and government identification numbers, financial account details and precise location.

Data protection laws means the laws that apply to the company responsible for your data and to you, including those listed in Part B.

4. The personal data we collect

The information we collect depends on how you deal with us. It is likely to include the following.

Enquiries and quotes

- Your name, title, email address, postal address and telephone numbers.
- Your travel preferences, interests, budget, travelling companions and the details of the trip you are considering.
- How you heard about us and any notes we take of our conversations with you.

Bookings and travel arrangements

- The lead passenger's name, contact details and, where different, the contact details of the person arranging or paying for the trip.
- The full name (as it appears on the passport), date of birth, gender, nationality and contact details of every traveller.

- Passport or national identity document details, visa information, frequent flyer and loyalty programme numbers, and known traveller or trusted traveller numbers, as required by airlines, cruise lines, immigration authorities and other suppliers.
- Emergency contact details and, for children, the name and contact details of a parent or guardian.
- Seating, room, bedding and other preferences.
- Special category data: dietary requirements, information about any medical condition, disability, allergy, pregnancy or reduced mobility that may affect anyone travelling, and requests for assistance. See section 7.
- Travel insurance details where you ask us to arrange insurance or a supplier requires evidence of it.
- Booking history, itineraries, correspondence, feedback and complaints.

Payments

- Billing name and address, invoices, payment amounts and dates, and confirmation of payment.
- Card and bank details are collected directly by our payment processor, or over the telephone or by secure form where we then pass them to the payment processor. We do not retain full card numbers on our own systems.

Membership and the 360 Juno portal

- Your login details, profile, stored traveller profiles, saved preferences and the itineraries, documents and messages available in your account.
- Records of your use of the portal, including access logs kept for security.

Marketing and events

- Your name and the contact details for the channels you have agreed to receive communications on, your communication preferences, and records of your responses to our newsletters, invitations and surveys.
- If you enter a competition, attend an event or take part in a survey, the details you give us for that purpose, and photographs or video taken at events where you have been told this will happen.

Websites, apps and social media

- Technical information such as your IP address, device type, browser, operating system, language, time zone, referring website and the pages you view, collected through cookies and similar technologies as described in section 17.
- Content you submit through our web forms, live chat or social media accounts, and your public social media profile information when you interact with our accounts.

Suppliers, partners and travel designers

- If you work for or with one of our suppliers or business partners, or apply to become a 360 Private Travel travel designer, we collect your business contact details, role, correspondence and the information needed to manage our relationship or your application.

Where we need personal data to fulfil a contract with you or to meet a legal requirement (for example passport details required by an airline or an immigration authority) and you do not provide it, we may be unable to make or complete the booking. We will tell you when this is the case.

5. Where we get your personal data from

Most of the personal data we hold comes directly from you or from the person arranging the trip on your behalf. If you are giving us information about other travellers, please make sure they know about this policy and that you are authorised to share their information, including any special category data.

We also receive personal data from: our travel designers, who are experienced travel professionals working through 360 Private Travel and bound by our confidentiality and data protection requirements; our group companies; hotels, airlines, cruise lines, tour operators, villa owners, ground handlers and other suppliers (for example booking confirmations, loyalty numbers and details of your stay); the Virtuoso network and other travel networks of which we are a member; travel insurance providers; payment processors and fraud prevention services; publicly available sources such as company websites and professional networking sites (business contacts only); and technology providers that support our websites and systems.

6. Why we use your personal data and our legal grounds

Data protection laws in most of the countries where we operate require us to have a legal ground for each use of your personal data. The table below sets out our purposes and the grounds we rely on. Where a purpose relies on our legitimate interests, we have assessed that our interests are not outweighed by your interests or rights; you can ask us for details of that assessment using the contact details in section 21.

What we use your personal data for	Legal ground
Responding to your enquiry, preparing a proposal or quote and negotiating a booking.	Taking steps at your request before entering into a contract; our legitimate interest in running our business and responding to people who contact us.
Making, changing and managing your booking, issuing tickets and travel documents, and providing the travel services you have bought, including passing details to suppliers.	Performance of our contract with you.
Providing your passport, identity and travel details to airlines, cruise lines, immigration, customs, border and security authorities (for example Advance Passenger Information).	Performance of our contract with you; compliance with legal obligations placed on us or on our suppliers.
Using information about health, disability, mobility, dietary and religious needs so that we and our suppliers can make suitable arrangements.	Your explicit consent. In an emergency, protection of your or another person's vital interests.
Taking payment, issuing invoices and refunds, keeping accounts, and complying with tax, financial protection (such as ATOL) and audit requirements.	Performance of our contract with you; compliance with legal obligations.
Providing your membership and the 360 Juno portal.	Performance of our contract with you.
Communicating with you before, during and after your trip, including travel alerts, emergency assistance and customer care.	Performance of our contract with you; our legitimate interest in looking after our clients; protection of vital interests in an emergency.
Sending you newsletters, offers, invitations and other marketing, and tailoring what we send to your interests.	Your consent, or, where the law allows, our legitimate interest in promoting our services to existing clients who have not opted out. See section 9.
Handling complaints, feedback, disputes and legal claims, and keeping records of our dealings with you.	Our legitimate interest in resolving issues and defending our rights; compliance with legal obligations.

What we use your personal data for	Legal ground
Keeping our systems, premises and information secure, preventing fraud and misuse, and verifying your identity when you exercise your rights.	Our legitimate interest in protecting our business and our clients; compliance with legal obligations. In the United Kingdom, the recognised legitimate interests of crime prevention and network security.
Improving our services, websites and portal, analysing how they are used and training our staff and travel designers.	Our legitimate interest in understanding and improving our business. Where analysis uses cookies, your consent (see section 17).
Managing our relationships with suppliers, partners and travel designers.	Performance of our contract with the relevant business; our legitimate interests in operating our business.
A sale, merger, reorganisation or financing of our business, or an insolvency process.	Our legitimate interest in running and structuring our business; compliance with legal obligations, including financial protection schemes.

In countries whose laws are based on consent rather than a list of legal grounds (for example the United Arab Emirates and, for some purposes, Hong Kong, Japan and Singapore), we rely on your consent, which you give by providing your details for the purposes described in this policy, or on the exceptions those laws allow. Part B explains this further.

7. Special category and sensitive data

Arranging travel sometimes means we need to know about health conditions, disabilities, reduced mobility, allergies, pregnancy, dietary requirements and religious observance, so that we and our suppliers can make the right arrangements and keep you safe. We only collect this information where it is relevant to the trip, and we will ask for your explicit consent when you give it to us. Where the information concerns another traveller, the person providing it confirms that they have that traveller's authority to share it. For children under 18, consent is given by a parent or guardian, or by the lead passenger with the parent's or guardian's authority.

We share special category data only with the suppliers who need it to provide the relevant service (for example an airline providing wheelchair assistance or a hotel catering for an allergy) and we delete it when it is no longer needed for the trip, as set out in section 13. You may withdraw your consent at any time, but if you do so we may not be able to make the arrangements you have asked for.

Passport and national identity numbers, financial account details and account login credentials are treated as sensitive data in some countries, including several US states. We use them only for the purposes described in this policy and protect them with additional security controls.

8. Children

Our services are aimed at adults. We collect information about children only where it is provided by a parent, guardian or the lead passenger for the purpose of a booking. We do not knowingly collect personal data directly from anyone under 18 (or a lower age where local law sets one, such as 13 in the United States and 16 in some EEA countries) without the consent of a parent or guardian. We do not send marketing to children. If you believe a child has provided us with personal data directly, please contact us and we will delete it.

9. Marketing

We would like to keep you informed about our services, destinations, offers and events by email, post, telephone, text message and messaging apps, and through our social media accounts. We will do this only where:

- you have consented, for example by ticking a box on our website, joining our membership, subscribing to a newsletter or telling your travel designer; or
- you are an existing client and local law allows us to send you information about similar services on an opt-out basis (for example the "soft opt-in" under the UK Privacy and Electronic Communications Regulations and the equivalent exceptions in the Netherlands and Switzerland).

Some countries require your prior opt-in for particular channels, including Australia (Spam Act 2003), Hong Kong (Part 6A of the Personal Data (Privacy) Ordinance), Singapore (Do Not Call Registry), the United Arab Emirates (telemarketing and SMS rules), the United States (text messages and automated calls under the TCPA) and the Netherlands (telemarketing). We comply with those rules and Part B gives more detail.

You can opt out at any time by using the unsubscribe link in any email, replying STOP to a text message, telling your travel designer, or emailing privacy@360privatetravel.com. You can choose which channels you are happy for us to use. We will act on your request promptly and in any event within the time limits that apply locally. Opting out of marketing does not stop us sending you service messages about your booking or membership.

We may use information about your bookings, preferences and how you respond to our communications to make sure what we send you is relevant. We do not sell your personal data to third parties for their own marketing, and we do not share it with third parties for targeted advertising.

10. Who we share your personal data with

We share personal data only where necessary for the purposes in section 6 and only the data needed for each purpose. Recipients include the following.

- **Travel suppliers.** Airlines and other transport providers, hotels, villas, resorts and other accommodation, cruise lines and yacht operators, tour operators, destination management companies, ground handlers, guides, chauffeurs, restaurants, insurers and any other supplier of services you book through us. Suppliers use your information under their own privacy policies, which we encourage you to read, particularly where a supplier is outside your home country.
- **Our group companies and travel designers.** The 360 Private Travel companies listed in section 2 and the travel designers who work with them, so that they can support your booking and provide you with a consistent service. Independent travel designers act on our behalf and are bound by written confidentiality and data protection obligations.
- **Travel networks.** Virtuoso and other travel networks of which we are a member, where this is needed to obtain the benefits and amenities available to you through those networks.
- **Service providers.** Companies that provide services to us, including booking and reservation systems, customer relationship management and email marketing platforms, payment processors, IT hosting, cloud storage, security and support, communications tools, document signing, accounting, insurance and professional advisers. Service providers act on our instructions under written contracts that require them to keep your data secure and confidential and to use it only to provide their services to us.
- **Payment processors and banks.** When you pay by card or bank transfer, your payment details are handled by our payment processor and our bank, who are independently responsible for that data under their own policies and are subject to the Payment Card Industry Data Security Standard.
- **Government and public authorities.** Immigration, customs, border, security, tax and other authorities where they require your information in connection with your travel (for example advance passenger information programmes, visa applications and health declarations), or where we are required by law, court order or regulatory request to disclose it.
- **Financial protection bodies and insolvency practitioners.** In the unlikely event of our insolvency, we or an appointed insolvency practitioner may disclose your booking information to the relevant financial

protection scheme, for example the UK Civil Aviation Authority under the ATOL scheme, so that it can assess the status of your booking and advise you. The CAA's privacy notice is at caa.co.uk.

- **Business transfers.** Prospective or actual purchasers, investors, lenders and their advisers in connection with a sale, merger, reorganisation or financing of our business, subject to confidentiality obligations.
- **Professional advisers and regulators.** Our lawyers, auditors, insurers and regulators where necessary to obtain advice, meet our obligations or establish, exercise or defend legal claims.

11. International transfers

We are an international business and travel is by its nature international. Your personal data will be transferred between our offices worldwide (see section 2 for the countries in which they are located), to suppliers in the destinations you visit, and to service providers whose systems may be hosted in other countries, including the United States and the EEA.

Some of these countries do not have data protection laws that are as strong as those in your own country. Where your data is transferred out of the country whose laws protect it, we take the steps that those laws require, which depending on the jurisdiction include one or more of the following:

- transferring only to countries that your regulator has recognised as providing adequate protection (for example the European Commission and the UK government recognise each other's regimes, the EEA, the United Kingdom and Switzerland recognise one another, and the EU-US, UK-US and Swiss-US Data Privacy Framework arrangements cover certified US organisations);
- putting in place contracts that impose data protection obligations on the recipient, including the European Commission's Standard Contractual Clauses, the UK International Data Transfer Agreement or Addendum, the Swiss-adapted Standard Contractual Clauses, the Hong Kong Recommended Model Contractual Clauses, the safeguards required under the Singapore, Japanese, Australian and UAE transfer rules, and our intra-group data transfer agreement covering all 360 Private Travel companies;
- relying, where the law permits, on the fact that the transfer is necessary to perform your booking (for example sending your details to a hotel in your destination), on your explicit consent after we have informed you of the risks, or on the need to protect someone's vital interests.

Where a transfer is necessary to provide the travel services you have booked, we cannot control the data protection standards of the destination country or the supplier there, and you accept that the transfer is a necessary part of your travel arrangements. You can ask us for more information about the safeguards we use, including a copy of the relevant contractual clauses, by contacting us at privacy@360privatetravel.com.

12. How we protect your personal data

We apply technical and organisational measures appropriate to the risk, including encryption of data in transit and at rest where supported, multi-factor authentication and role-based access to our systems, secure cloud hosting with reputable providers, regular backups, staff and travel designer training, confidentiality obligations, supplier due diligence, and procedures for identifying, containing and reporting security incidents. Passport images and other sensitive documents are stored in secure systems with restricted access and are not sent by unsecured means where a secure alternative is available.

No transmission over the internet is completely secure. If you receive an email that appears to come from us and asks for payment to a new bank account or for your card details, please telephone your travel designer on a known number before acting on it.

13. How long we keep your personal data

We keep personal data only for as long as necessary for the purposes it was collected for, including to meet legal, accounting, financial protection and reporting requirements and to deal with any complaints or claims. Our standard retention periods are:

Type of data	How long we keep it
Booking records, itineraries, invoices and payment records	7 years from the end of the trip (or longer if required by local tax or company law), to meet accounting, tax, financial protection and limitation period requirements.
Passport and identity document copies and numbers	For the duration of the booking and no longer than 12 months after the trip ends, unless you ask us to keep them on your traveller profile for future bookings, in which case until you ask us to delete them or your account has been inactive for 3 years.
Special category data (health, dietary, mobility, religious requirements)	Deleted within 3 months after the trip ends, unless you ask us to keep it on your profile for future bookings or it is needed for a complaint or claim.
Enquiries and quotes that do not become a booking	24 months from our last contact with you.
Membership and 360 Juno accounts	For the life of your membership and 2 years afterwards, except for data we must keep longer under the rows above.
Marketing consents and preferences	Until you withdraw consent or opt out, and we keep a record of your opt-out so that we can respect it. We review inactive marketing contacts every 3 years.
Correspondence, complaints and claims	7 years from resolution, or longer if a claim is ongoing.
Website and portal logs and analytics	Security logs up to 12 months; analytics data in aggregated or pseudonymised form as described in our cookie notice.
Supplier, partner and travel designer contacts	For the duration of our relationship and 7 years afterwards for contractual and accounting purposes.

When data is no longer needed we delete it securely or anonymise it so that it can no longer be linked to you. Some countries in Part B require us to tell you about retention in a particular way, and we have done so there.

14. Automated decision-making and profiling

We do not make decisions about you based solely on automated processing that produce legal effects or similarly significant effects for you. Our travel designers make the decisions about your travel arrangements. We may use software to segment our marketing audience (for example by destination interest or booking history) and to detect fraud or security threats; these tools support decisions made by people. If we introduce automated decision-making of a kind that the law requires us to tell you about, we will update this policy and, where required, obtain your consent.

We may use artificial intelligence tools to help draft itineraries, summarise correspondence and support our staff. Where we do so, we use tools under contracts that prohibit the provider from using your personal data to train their models, and we do not enter special category data into such tools unless the tool is provided under a contract that meets our security requirements.

15. Your rights

Depending on where you live and which company is responsible for your data, you have some or all of the following rights. Part B sets out country-specific variations.

- **Access.** To be told whether we hold personal data about you and to receive a copy of it, together with information about how we use it.
- **Correction.** To have inaccurate or incomplete personal data corrected.
- **Deletion.** To have your personal data deleted in certain circumstances, for example where it is no longer needed or you have withdrawn consent, subject to our legal retention obligations.
- **Restriction.** To ask us to limit how we use your personal data in certain circumstances, for example while a dispute about accuracy is resolved.
- **Portability.** To receive the personal data you gave us in a structured, commonly used, machine-readable format and to have it transmitted to another organisation, where the law provides this right.
- **Objection.** To object to processing based on our legitimate interests, and to object at any time to direct marketing and to profiling for marketing.
- **Withdrawal of consent.** To withdraw any consent you have given, without affecting the lawfulness of processing before withdrawal.
- **Automated decisions.** Not to be subject to a decision based solely on automated processing that has legal or similarly significant effects, and to ask for human review.
- **Complaint.** To complain to us and to the relevant regulator (see section 16).
- **No discrimination.** Not to be treated differently because you have exercised your rights.

To exercise any right, email privacy@360privatetravel.com or write to the address of the relevant company in section 2, or ask your travel designer. We may need to confirm your identity and, if you are acting for someone else, your authority to do so. We do not charge a fee unless the law allows it and a request is clearly unfounded, repetitive or excessive. We will respond without undue delay and within the time limit that applies where you live: one month in the United Kingdom, the EEA and Switzerland (extendable by two further months for complex or numerous requests, and in the United Kingdom the clock may pause while we ask you for information we reasonably need to identify what you are asking for); 30 days in Australia, Singapore and Japan (or as soon as reasonably practicable); 40 days in Hong Kong; and 45 days in the United States (extendable by 45 days). Some rights are subject to exceptions, and if we cannot comply with a request we will explain why.

16. Complaints

If you are unhappy with how we have handled your personal data, please tell us first so that we can put things right. Email privacy@360privatetravel.com with the word "Complaint" in the subject line, or write to the relevant company at the address in section 2. We will acknowledge your complaint within 30 days, investigate it, keep you informed and tell you the outcome without undue delay. This procedure is available free of charge.

You also have the right to complain to a data protection regulator, in particular the regulator in the country where you live, work or where you believe a breach occurred. The regulators for the countries where we have offices are:

Country	Regulator	How to contact
United Kingdom	Information Commissioner's Office (ICO)	ico.org.uk/make-a-complaint , helpline 0303 123 1113
Netherlands and other EEA countries	Autoriteit Persoonsgegevens (or the supervisory authority of the EEA country where you live or work)	autoriteitpersoonsgegevens.nl

Country	Regulator	How to contact
Switzerland	Federal Data Protection and Information Commissioner (FDPIC)	edoeb.admin.ch
Australia	Office of the Australian Information Commissioner (OAIC)	oaic.gov.au
Hong Kong	Office of the Privacy Commissioner for Personal Data (PCPD)	pcpd.org.hk, +852 2827 2827
Japan	Personal Information Protection Commission (PPC)	ppc.go.jp
Singapore	Personal Data Protection Commission (PDPC)	pdpc.gov.sg
United Arab Emirates	The competent federal data protection authority (currently the Federal Authority for Artificial Intelligence and Data, successor to the UAE Data Office)	uaelegislation.gov.ae
United States	Your state Attorney General, the Federal Trade Commission and, for California residents, the California Privacy Protection Agency	ftc.gov, privacy.ca.gov

17. Cookies and similar technologies

Our websites and portal use cookies, pixels, local storage and similar technologies. Some are strictly necessary for the site to work, for example to keep you logged in, remember your cookie choices and protect against fraud; these do not require your consent. Others help us understand how the site is used, remember your preferences, or measure and personalise our marketing; we use these only with your consent, which you can give or refuse through the cookie banner when you first visit and change at any time through the cookie settings link on the site or your browser settings. Refusing non-essential cookies will not stop you using the site, though some features may work less well. We do not use cookies that would amount to selling or sharing your personal data for targeted advertising by third parties.

Our cookie notice, available on each website, lists the cookies we use, what they do, who sets them and how long they last. Where we use analytics or advertising services provided by third parties, those providers may receive your IP address and browsing information and may use it in accordance with their own policies; the cookie notice identifies them.

Where we send you emails, we may use technology that tells us whether the email was opened and which links were clicked, so that we can measure and improve our communications. You can prevent this by disabling images in your email client or by unsubscribing.

18. Links to other websites and supplier policies

Our websites and communications may contain links to websites operated by suppliers, partners and other third parties. We are not responsible for the privacy practices of those websites, and this policy does not apply to them. Suppliers who provide your travel services are separately responsible for the personal data they receive, and their privacy policies apply to that data.

19. Personal data breaches

We have procedures for identifying, containing, assessing and recording security incidents involving personal data. Where the law requires it, we will notify the relevant regulator within the applicable deadline (for example 72 hours in the United Kingdom and the EEA, 3 calendar days in Singapore, and as soon as practicable

in Australia, Japan and Switzerland) and we will tell you if the breach is likely to result in a high risk to you, or where local law otherwise requires, so that you can take steps to protect yourself.

20. Changes to this policy

We review this policy at least once a year and whenever the law, regulatory guidance or our practices change. The current version, with its effective date, is always available on our website. Where a change materially affects how we use your personal data, we will tell you by email or through the portal before it takes effect, and where the law requires it we will ask for your consent.

21. How to contact us

Our privacy team can be reached at:

- Email: privacy@360privatetravel.com
- Post: Privacy Team, 360 Private Travel Limited, 54 High Street, Sevenoaks, Kent TN13 1JG, United Kingdom, or the address of the relevant group company in section 2
- Telephone: +44 207 434 2244

You can also raise any privacy question with your travel designer, who will pass it to the privacy team.

Part B. Additional information for each country where we operate

This Part applies in addition to Part A. Where there is any inconsistency, the provisions of this Part that apply to you take precedence.

B1. United Kingdom

Controller: 360 Private Travel Limited, 54 High Street, Sevenoaks, Kent TN13 1JG (company number 08512928), registered with the Information Commissioner's Office as a fee payer and the holder of ATOL licence 7514.

Law: the UK General Data Protection Regulation and the Data Protection Act 2018, each as amended by the Data (Use and Access) Act 2025, and the Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR).

Lawful bases: section 6 sets out the lawful bases we rely on under Article 6 UK GDPR. For special category data we rely on your explicit consent (Article 9(2)(a)) and, in an emergency, the protection of vital interests (Article 9(2)(c)). Where we rely on the recognised legitimate interests introduced by the 2025 Act (for example preventing crime or securing our networks) no balancing test is required; for all other legitimate interests we have carried out a legitimate interests assessment.

Marketing: we send email and text marketing to existing clients under the PECR "soft opt-in" only where we obtained your details in the course of a sale or negotiations for a sale, the marketing concerns our similar services, and you were given a simple opportunity to refuse at the time and in every message. Otherwise we ask for your consent. We screen telephone marketing against the Telephone Preference Service.

Your requests: we respond to subject access and other rights requests within one month. The 2025 Act allows us to pause that period while we ask you for information we reasonably need to clarify your request, and requires us to carry out a reasonable and proportionate search. We may extend the period by up to two further months for complex or multiple requests and will tell you if we do.

Complaints: you have the right to complain to us, and we operate the complaints procedure described in section 16, acknowledging complaints within 30 days as the 2025 Act requires. You also have the right to complain to the Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF, ico.org.uk, helpline 0303 123 1113.

International transfers: transfers from the United Kingdom are made under UK adequacy regulations (which cover the EEA, Switzerland, Japan and, for certified organisations, the United States under the UK-US Data Bridge), the UK International Data Transfer Agreement or Addendum, or the exceptions in Article 49 UK GDPR, having applied the data protection test required by the 2025 Act.

Financial protection: many of the flights and flight-inclusive holidays we arrange are financially protected by the ATOL scheme. In the event of our insolvency, we or an insolvency practitioner may share your booking details with the Civil Aviation Authority so that it can administer the scheme. The CAA's privacy notice is at caa.co.uk.

Cookies: under PECR as amended, we may set cookies that are strictly necessary, and certain low-risk statistical, appearance and preference cookies, without consent, provided we tell you about them and give you a simple way to object. All other cookies are set only with your consent.

B2. Netherlands and the European Economic Area

Controller: 360 Private Travel B.V., Spaces Westerpark, Haarlemmerweg 331, 1051 LH Amsterdam (KvK 76863492), a member of the ANVR (number 5749). Clients served by our team in Paris contract with 360 Private Travel B.V. unless their booking confirmation names another group company.

Law: Regulation (EU) 2016/679 (the GDPR), the Dutch GDPR Implementation Act (Uitvoeringswet AVG) and the Dutch Telecommunications Act (Telecommunicatiewet), together with the data protection and e-privacy laws of any other EEA country in which you live.

Lawful bases: as set out in section 6, under Article 6 GDPR, and Article 9(2)(a) and (c) for special category data. Where you live in the EEA but contract with a 360 Private Travel company outside the EEA, that company processes your data on the same bases and you retain your rights under the GDPR.

Marketing: under Article 11.7 of the Telecommunications Act we send electronic marketing only with your prior consent, except that we may email existing clients about our own similar services provided you were given an opportunity to object when your details were collected and in each message. Telephone marketing to consumers requires your prior consent. You have an absolute right to object to direct marketing under Article 21(2) GDPR.

Cookies: under Article 11.7a of the Telecommunications Act we place cookies that are not strictly necessary or purely analytical with minimal privacy impact only after you have given consent through a banner that lets you accept or reject with equal ease. We do not use cookie walls.

International transfers: transfers outside the EEA are made under European Commission adequacy decisions (including those for the United Kingdom, Switzerland, Japan and, for certified organisations, the EU-US Data Privacy Framework), the Standard Contractual Clauses adopted under Commission Decision (EU) 2021/914 with any supplementary measures our transfer risk assessment requires, or the derogations in Article 49 GDPR. Because the Data Privacy Framework is subject to a pending court challenge, we also maintain Standard Contractual Clauses with our principal US service providers.

Complaints: you may complain to the Autoriteit Persoonsgegevens, Postbus 93374, 2509 AJ Den Haag, autoriteitpersoonsgegevens.nl, or to the supervisory authority of the EEA country where you live or work.

Representative and DPO: as 360 Private Travel B.V. is established in the EEA, no Article 27 representative is required. We have not appointed a statutory data protection officer because our core activities do not involve large-scale monitoring or large-scale processing of special category data; our privacy team is responsible for data protection and can be contacted as set out in section 21.

B3. Switzerland

Controller: 360 Private Travel AG, Bellerivestrasse 203, 8008 Zürich (CHE-210.327.509).

Law: the Federal Act on Data Protection of 25 September 2020 (FADP), in force since 1 September 2023, the Data Protection Ordinance (DPO) and, for electronic marketing, Article 3(1)(o) of the Federal Act against Unfair Competition.

Information under Article 19 FADP: the identity and contact details of the controller are above; the purposes of processing are in section 6; the recipients or categories of recipients are in section 10. Personal data is disclosed abroad to the countries in which our group companies are located (see section 2), to suppliers in your destination countries, and to service providers in the United States and the EEA. The United Kingdom, EEA countries and (for certified organisations) the United States under the Swiss-US Data Privacy Framework are recognised by the Federal Council as providing adequate protection. For other countries we rely on the Standard Contractual Clauses as adapted for Switzerland, our intra-group agreement, or the exceptions in Article 17 FADP, in particular where the transfer is necessary to perform your booking.

Sensitive personal data: health data, data on religious views and biometric data are sensitive personal data under the FADP. We process them only with your express consent or where necessary to protect your life or physical integrity.

Your rights: you have the rights of access (Article 25), rectification (Article 32), data portability (Article 28), and to object to or restrict processing, as described in section 15. Rights are enforced through the civil courts; the

Federal Data Protection and Information Commissioner (FDPIC), Feldeggweg 1, 3003 Bern, edoeb.admin.ch, may also receive reports and investigate.

Marketing: we send mass advertising by email or text only with your prior consent or, for existing clients, where we obtained your details in the course of a sale, the advertising concerns our similar services and each message offers a free and simple way to opt out. Every message identifies us as the sender.

Breaches: we notify the FDPIC as soon as possible of any breach likely to result in a high risk to your personality or fundamental rights, and we inform you where this is necessary for your protection or the FDPIC requests it.

B4. Australia

Controller (APP entity): 360 Private Travel Pty Ltd, Level 5, 179 Elizabeth Street, Sydney NSW 2000 (ABN 93 685 913 071). We comply with the Australian Privacy Principles (APPs) whether or not we would otherwise fall within a small business exemption.

Law: the Privacy Act 1988 (Cth), including the APPs and the Notifiable Data Breaches scheme, as amended by the Privacy and Other Legislation Amendment Act 2024; the Spam Act 2003 (Cth); and the Do Not Call Register Act 2006 (Cth).

Collection (APP 3 and 5): the kinds of personal information we collect and hold, and how we collect and hold them, are described in sections 4, 5 and 12. We collect personal information directly from you where reasonably practicable. Sensitive information (including health information and information about religious beliefs) is collected only with your consent and where reasonably necessary for the travel arrangements. If you do not provide the information we need, we may not be able to arrange your travel.

Use and disclosure (APP 6): we use and disclose personal information for the primary purpose of arranging and providing your travel and related purposes you would reasonably expect, as described in section 6.

Direct marketing (APP 7 and the Spam Act): we send commercial electronic messages only with your express or inferred consent, each message identifies us and contains a functional unsubscribe facility, and we act on unsubscribe requests within 5 business days. You may at any time ask us not to send you direct marketing and to tell you where we obtained your information.

Overseas disclosure (APP 8): we are likely to disclose your personal information to overseas recipients, in particular to our other group companies (see section 2 for the countries in which they are located), to travel suppliers in the countries you visit, and to service providers hosted in the United States and the EEA. Before disclosing personal information overseas we take reasonable steps to ensure the recipient handles it in accordance with the APPs, or we rely on your informed consent or another exception in APP 8.2.

Automated decision-making (APP 1.7 to 1.9, applying from 10 December 2026): we do not use computer programs to make decisions that could reasonably be expected to significantly affect your rights or interests, or to do a thing that is substantially and directly related to such a decision. If this changes, we will describe here the kinds of personal information used and the kinds of decisions involved.

Access, correction and complaints (APP 1, 12 and 13): you may request access to or correction of your personal information through the contact details in section 21. We will respond within 30 days. If you have a complaint about our handling of your personal information, please raise it with us first; we will acknowledge it promptly and aim to resolve it within 30 days. If you are not satisfied, you may complain to the Office of the Australian Information Commissioner, GPO Box 5288, Sydney NSW 2001, oaic.gov.au, 1300 363 992.

Data breaches: if a data breach is likely to result in serious harm to you, we will notify you and the OAIC as soon as practicable in accordance with the Notifiable Data Breaches scheme.

B5. Hong Kong

Data user: 360 Private Travel Limited, Units 1001-03, 10/F, Prosperity Millennia Plaza, 663 King's Road, Quarry Bay, Hong Kong (business registration 71239999-000-10-20-A; Travel Industry Authority licence 354498).

Law: the Personal Data (Privacy) Ordinance (Cap. 486) (PDPO), including the six Data Protection Principles and Part 6A on direct marketing.

Personal Information Collection Statement (DPP1(3)): this section, together with Part A, is our Personal Information Collection Statement. It is your choice whether to provide personal data to us; however, if you do not provide the data we need to make a booking (such as traveller names, dates of birth and passport details), we will not be able to arrange your travel. The purposes for which your data will be used are set out in section 6. The classes of persons to whom your data may be transferred are set out in section 10, and include our group companies, travel suppliers, service providers, travel networks and government authorities. You have the right to request access to and correction of your personal data under sections 18 and 22 of the PDPO, and requests should be sent to the Privacy Team at privacy@360privatetravel.com or to the address above. We may charge a reasonable fee for complying with a data access request. We will respond within 40 days.

Direct marketing (Part 6A): before using your personal data in direct marketing for the first time, we will tell you that we intend to do so, the kinds of personal data to be used (your name and contact details), the classes of services to be marketed (luxury travel, membership, events and related services), and that you may opt out free of charge. We will not use your personal data in direct marketing unless you have indicated that you do not object, and we will not provide your personal data to any other person for use in their direct marketing. You may ask us to stop using your personal data in direct marketing at any time.

Transfers outside Hong Kong: section 33 of the PDPO is not yet in operation, but we treat transfers outside Hong Kong in accordance with the Privacy Commissioner's guidance and, where practicable, adopt the Recommended Model Contractual Clauses. Your data may be transferred to the places listed in section 11.

Retention (DPP2): we retain personal data no longer than necessary for the purposes described in section 13.

Data breaches: although notification is not currently mandatory in Hong Kong, we will notify the Privacy Commissioner and affected individuals as soon as practicable where a breach is likely to cause a real risk of harm, in line with the Commissioner's guidance.

Complaints: you may complain to the Office of the Privacy Commissioner for Personal Data, Unit 1303, 13/F, Dah Sing Financial Centre, 248 Queen's Road East, Wanchai, Hong Kong, pcpd.org.hk, +852 2827 2827.

B6. Japan

Business operator handling personal information: 360 Private Travel K.K., 8F Shinkawa Ohara Building, 1-27-8 Shinkawa, Chuo-ku, Tokyo 104-0033 (corporate number 0100-01-244642). Representative: James Turner, Representative Director.

Law: the Act on the Protection of Personal Information (Act No. 57 of 2003) (APPI), as amended, and the rules and guidelines of the Personal Information Protection Commission. Marketing emails are also governed by the Act on Regulation of Transmission of Specified Electronic Mail. The amendment to the APPI promulgated in July 2026 will take effect in stages, and we will update this section when it does.

Purposes of use (Article 21): the purposes for which we use personal information are specified in section 6. We will not use personal information beyond the scope necessary for those purposes without your prior consent, and we will not use it in a way that may encourage or induce unlawful or unjust acts.

Sensitive personal information: we obtain your prior consent before acquiring information requiring special care, such as health information, except where the law allows otherwise.

Provision to third parties (Article 27): we provide personal information to third parties, including travel suppliers and service providers, where necessary to perform your booking and with your consent, which you give by requesting the booking, or where an exception under the APPI applies (for example where provision is necessary to protect life or physical safety). We keep the records of third-party provision that the APPI requires. We do not rely on the opt-out procedure under Article 27(2).

Joint use (Article 27(5)(iii)): personal information may be used jointly by the 360 Private Travel group companies listed in section 2. The items used jointly are the categories listed in section 4; the joint users are those group companies; the purpose of joint use is the purposes in section 6; and the entity responsible for managing the jointly used data, including its name and address, is 360 Private Travel K.K. at the address above (for clients of the Japan office) or the group company responsible for your booking.

Provision to third parties in foreign countries (Article 28): your personal information may be provided to group companies, suppliers and service providers in the countries listed in section 11. Where the recipient is in a country that the Commission has designated as having an equivalent system (the United Kingdom and the EEA), or has established a system that meets the Commission's standards (including through our intra-group agreement and contractual safeguards, which we monitor), no separate consent is required. In other cases we obtain your consent after informing you of the name of the country, an outline of its personal information protection system and the measures taken by the recipient; you may request this information at any time through the contact in section 21.

Security control measures (Article 23): we have established internal rules and appointed a person responsible for handling personal information, train our staff, control access to personal information through authentication and role-based permissions, protect our systems against unauthorised access and malware, and confirm the data protection systems of foreign countries where we store or process data. Further details are available on request.

Disclosure, correction and suspension of use (Articles 33 to 35): you may request disclosure of your retained personal data (including records of third-party provision), correction, addition or deletion, and suspension of use or of provision to third parties. Send requests to privacy@360privatetravel.com; we will verify your identity and respond without delay, normally within 30 days. We may charge a reasonable fee for disclosure requests.

Complaints and the regulator: complaints about our handling of personal information should be sent to the contact in section 21. You may also contact the Personal Information Protection Commission, ppc.go.jp.

B7. Singapore

Organisation: 360 Private Travel Pte. Ltd., 22 Malacca Street, #03-02, RB Capital Building, Singapore 048980 (UEN 202003026H; Singapore Tourism Board travel agent licence TA03387).

Law: the Personal Data Protection Act 2012 (PDPA), the Personal Data Protection Regulations 2021, the Do Not Call provisions in Part 9 of the PDPA and the Spam Control Act 2007.

Data Protection Officer: our Data Protection Officer can be contacted at privacy@360privatetravel.com or on +65 3163 4421, or by post at the address above.

Consent and purposes: we collect, use and disclose personal data for the purposes notified in section 6 with your consent, which may be express, or deemed by conduct (for example when you voluntarily provide your details to make a booking), by notification (where we have told you of a new purpose and you have not opted out within a reasonable period) or by contractual necessity. We also rely, where appropriate, on the legitimate interests and business improvement exceptions in the First Schedule to the PDPA. You may withdraw consent at any time by giving us reasonable notice, and we will tell you the likely consequences of doing so.

Do Not Call Registry: we will not send marketing messages to a Singapore telephone number by voice call, text or fax unless we have checked the Do Not Call Registry within the previous 30 days and the number is not

listed, or you have given us clear and unambiguous consent to receive such messages. Every message will identify us and, for text messages, provide a way to opt out.

Transfers outside Singapore: we transfer personal data outside Singapore only where we have taken appropriate steps to ensure the recipient is bound by legally enforceable obligations to provide a standard of protection comparable to the PDPA, for example through our intra-group agreement or contractual clauses, or where you have consented after being informed of the position, or where the transfer is necessary to perform your booking.

Access and correction: you may request access to or correction of your personal data, and information about how it has been used or disclosed in the past year, through the DPO. We will respond within 30 days or tell you when we expect to respond. We may charge a reasonable fee for access requests.

Retention: we cease to retain documents containing personal data, or anonymise them, as soon as the purpose for collection is no longer served by retention and retention is no longer necessary for legal or business purposes, in accordance with section 13.

Data breaches: we assess suspected breaches promptly and, where a breach is likely to result in significant harm to affected individuals or involves 500 or more individuals, notify the Personal Data Protection Commission within 3 calendar days of that assessment and notify affected individuals unless an exception applies.

Complaints: if you are not satisfied with our response, you may complain to the Personal Data Protection Commission, 10 Pasir Panjang Road, #03-01 Mapletree Business City, Singapore 117438, pdpc.gov.sg.

B8. United Arab Emirates

Controller: 360 Private Travel L.L.C-FZ, Meydan Grandstand, 6th Floor, Meydan Road, Nad Al Sheba, Dubai (licence 2533992.01). Meydan Free Zone is not a financial free zone, so the federal data protection law applies rather than the DIFC or ADGM regimes.

Law: Federal Decree-Law No. 45 of 2021 on the Protection of Personal Data (PDPL) and its executive regulations when issued; Cabinet Resolution No. 56 of 2024 on the regulation of telemarketing; and the Telecommunications and Digital Government Regulatory Authority's rules on unsolicited electronic communications.

Consent and legal bases: under the PDPL we process your personal data on the basis of your consent, which must be clear, specific and freely given and which you may withdraw at any time, except where the PDPL allows processing without consent, including where processing is necessary to perform a contract with you, to comply with a legal obligation, to protect your interests, or for our legitimate interests that do not conflict with your rights. Section 6 identifies which basis we rely on for each purpose. Health data and other sensitive data are processed only with your explicit consent or where necessary to protect life.

Information under Article 13 PDPL: the purposes of processing are in section 6; the sectors and recipients, inside and outside the UAE, with whom your data may be shared are in section 10; the safeguards for cross-border transfers are in section 11; and your rights are in section 15, including the rights to access, correction, erasure, restriction, portability, objection to processing (including direct marketing and profiling) and in relation to automated decision-making.

Cross-border transfers (Articles 22 and 23 PDPL): as no adequacy decisions have yet been issued under the PDPL, we transfer personal data outside the UAE under contracts that bind the recipient to standards equivalent to the PDPL (including our intra-group agreement), with your explicit consent, or where the transfer is necessary to perform your booking or to protect your vital interests.

Marketing: we send marketing by text message, messaging app or social media only with your prior consent, and any telemarketing calls are made in accordance with Cabinet Resolution No. 56 of 2024, including checking

the Do Not Call Register and calling only between 9 am and 6 pm. Every message identifies us and offers an easy way to opt out.

Data breaches: we will notify the competent authority and, where a breach is likely to result in a high risk to your privacy, notify you, within the periods set by the PDPL and its regulations.

Regulator and complaints: complaints should first be raised with us under section 16. You may also complain to the competent federal data protection authority (at the date of this policy, the Federal Authority for Artificial Intelligence and Data, which has succeeded the UAE Data Office) and, for telemarketing and spam, to the Telecommunications and Digital Government Regulatory Authority.

B9. United States

Controller (business): 360 Private Travel LLC, 1688 Meridian Avenue, Suite 00, Miami Beach, FL 33139 (Florida Seller of Travel Registration No. ST 700358).

Law: the privacy laws of the state in which you live, which may include the California Consumer Privacy Act as amended by the California Privacy Rights Act (CCPA) and the comprehensive consumer privacy laws in force in Colorado, Connecticut, Delaware, Florida, Indiana, Iowa, Kentucky, Maryland, Minnesota, Montana, Nebraska, New Hampshire, New Jersey, Oregon, Rhode Island, Tennessee, Texas, Utah and Virginia, among others; the federal CAN-SPAM Act, Telephone Consumer Protection Act (TCPA) and Children's Online Privacy Protection Act (COPPA); and Florida's Information Protection Act and Sellers of Travel Act. Many of these laws apply only to businesses above certain size thresholds. Whether or not a particular law applies to us, we extend the rights in this section to all US residents.

Categories of personal information we have collected in the past 12 months: identifiers (name, postal address, email address, telephone number, passport number, account name, IP address); customer records (billing details, signature); protected classifications (date of birth, gender, nationality and, where you tell us, disability or religion for dietary purposes); commercial information (bookings, itineraries, purchase history, preferences); internet or network activity (interactions with our websites, portal and emails); audio or visual information (call recordings where notified, event photographs); inferences drawn from the above to personalise our service and communications; and sensitive personal information (passport and government identification numbers, account log-in credentials, health information, and racial, ethnic or religious information disclosed through dietary or assistance requests). The sources of this information are described in section 5, the business purposes in section 6, and the categories of third parties to whom it is disclosed in section 10. Retention periods are set out in section 13.

Sale, sharing and targeted advertising: we do not sell your personal information and we do not share it for cross-context behavioural or targeted advertising, and we have not done so in the past 12 months. We have no actual knowledge that we sell or share the personal information of consumers under 16. We use sensitive personal information only for the purposes permitted without an opt-out right, namely to provide the services you request, to prevent fraud and security incidents and to comply with law; where a state requires opt-in consent for sensitive data, we obtain it at collection. Because we do not sell or share personal information, we do not provide a "Do Not Sell or Share" link, but we honour Global Privacy Control signals as a request to opt out of any sale or sharing.

Your rights: you may request to know or access the personal information we hold about you (including the specific pieces and, for California residents, the categories of sources and third parties), to obtain a portable copy, to correct inaccurate information, to delete your personal information, to opt out of any sale, sharing, targeted advertising or profiling in furtherance of decisions producing legal or similarly significant effects, and to limit the use of sensitive personal information. We will not discriminate against you for exercising your rights. To submit a request, email privacy@360privatetravel.com, call +1 312 724 5794 or write to the address above. We will verify your identity by matching the information you provide with our records and may ask for additional information; an authorised agent may submit a request on your behalf with your written permission.

We will respond within 45 days, extendable once by a further 45 days where reasonably necessary, and will tell you if we need more time.

Appeals: if we decline to act on your request, you may appeal by emailing privacy@360privatetravel.com with "Appeal" in the subject line within 45 days of our decision. We will respond in writing within 45 days with the reasons for our decision. If your appeal is denied, you may contact your state Attorney General; California residents may contact the California Privacy Protection Agency at privacy.ca.gov.

Marketing communications: our commercial emails comply with CAN-SPAM, identify us, include our postal address and an opt-out that we honour within 10 business days. We send marketing text messages or place automated or pre-recorded marketing calls only with your prior express written consent, which you may revoke at any time by any reasonable means, including replying STOP; message and data rates may apply. We honour the National Do Not Call Registry.

Children: we do not knowingly collect personal information online from children under 13. Information about child travellers is provided by their parents or guardians as part of a booking.

Florida: 360 Private Travel LLC is registered with the Florida Department of Agriculture and Consumer Services as a Seller of Travel (Fla. Seller of Travel Ref. No. ST 700358). In the event of a breach of security affecting your personal information as defined in the Florida Information Protection Act, we will notify you without unreasonable delay and within 30 days of determining the breach occurred, and we will notify the Florida Department of Legal Affairs where required.

Nevada, and other state notices: we do not sell covered information as defined in Nevada law. Residents of other states with privacy laws have the rights set out above to the extent provided by their state's law.

Summary of changes from the August 2022 policy

This section is provided for transparency and may be retained or removed at publication.

- Scope extended from the United Kingdom company alone to all 360 Private Travel operating companies worldwide, with a table (section 2) identifying which company is responsible for your data and a Part B section for each country.
- United Kingdom section updated for the Data (Use and Access) Act 2025, including recognised legitimate interests, the new subject access request rules, the statutory complaints procedure, the international transfer data protection test and the revised cookie rules.
- New sections on membership and the 360 Juno portal, travel designers, travel networks, artificial intelligence tools, automated decision-making, personal data breaches and children.
- Legal grounds for each purpose set out in a table, replacing the narrative description.
- Retention periods stated for each category of data.
- International transfers section rewritten to reflect the current adequacy decisions, the EU-US, UK-US and Swiss-US Data Privacy Frameworks, the Standard Contractual Clauses and the UK International Data Transfer Agreement, and the transfer rules of each Asia-Pacific, Middle East and US jurisdiction.
- Marketing section updated to reflect opt-in requirements in Australia, Hong Kong, Singapore, the UAE and the United States, and confirmation that personal data is not sold or shared for targeted advertising.
- Cookie section updated to reflect consent requirements and the UK's new consent exemptions.
- Single privacy contact (privacy@360privatetravel.com) and a regulator table covering every country of operation.
- Previous solicitors' copyright notice removed.