



Aethos Privacy Policy

Last updated: 27 July 2026

1. About us

Aethos AG, Landis + Gyr - Strasse 1, CH-6300 Zug, Switzerland is the owner, and operator of Aethos' app and the website at Aethos.com. Aethos AG is a controller of personal data processed on our app and our website.

Our group companies are also controllers of personal data:

- processed in connection with the Aethos Members' Club; and/or
- processed when you are onsite at one of our hotels or clubs.

These group companies are set out by location in the table below.

For the Aethos Members' Club (if you are a member) the relevant controller will be the company in your home location selected by you when you apply for membership, and the entity that issues your membership fee invoices/receipts.

In respect of our hotels and clubs, the relevant controller will be the relevant company in the same location as the hotel or club that you are visiting.

Each controller can be contacted via hello@aethos.com in the first instance.

Location	Company
London, UK	Shoreditch OpCo Limited
Milan, Italy	The Yard S.R.L.
Palma, Mallorca, Spain	• <u>Hotel</u>: Development Palmira, S.L. • <u>Palma Club (membership)</u>: Asociación Club Sociocultural Morei, Palma, Spain • <u>Palma Club (other charges)</u>: Morei Members, Palma, Spain
Lisbon, Portugal	<u>Club</u> : Original Hospitality – Exploração Turística Unipessoal LDA
Ericeira, Portugal	<u>Hotel</u> : Praia Da Calada Hotel, LDA
Saragano, Gualdo Cattaneo, Italy	Borgo Sarano S.R.L.
Monterosa, Ayas, Italy	Regina Delle Alpi S.R.L.
Arzachena, Sardinia, Italy	Sardegna Smeralda S.R.L.

In this Privacy Policy references to "we," "our," or "us" means Aethos AG, or the relevant Aethos group company.

Please read this Privacy Policy, as it explains how we collect, use, and share your personal data.

2. How we collect your personal data



We collect your personal data from you:

- directly, such as when you book and pay for experiences, buy an e-gift card, subscribe to our newsletter, register for Aethos Members' Club, stay at one of our hotels, visit one of our clubs, connect with your concierge service, apply for a job via our website, or fill in a contact form on our website or app; and
- indirectly, when browsing our website or app, using cookies and other technologies referenced in section 7. below.

We also collect your personal data from other sources, as follows:

- travel agencies;
- booking platforms;
- other Aethos group companies, as listed above; and
- social media (for example if you contact us via social media).

3. Personal data that we collect

We may collect, store and use the following types of your personal data:

- **Booking Data:** information about which of our hotels you have stayed at, or are staying at and which of our clubs you have visited.
- **Candidate Data:** information included in a CV for example, prior employment, current employment, education and/or qualification and details of your social media profiles and/or websites (if you choose to provide these in support of a job application).
- **Communication Data:** personal data contained in or relating to any communication that you send to us or that we send to you, (including the communication content and metadata associated with the communication and any information gathered on a form).
- **Contact Data:** your telephone number(s), address and email address.
- **Health Data:** information about your medical conditions, allergies and intolerances.
- **Identity Data:** your name, title, date of birth, gender, marital status, passport number and data, nationality and place of birth, and employer details - for corporate hotel/club bookings.
- **Location Data:** your current location as disclosed by [GPS technology] for the time period where you have permitted us to collect it.
- **Marketing Data:** your preferences in receiving marketing from us and third parties, and records of marketing received from us.
- **Membership Data:** your username and password, membership level, benefits entitlement, interests, preferences, and feedback.
- **Technical Data:** internet protocol (IP) address, browser type and version, time zone setting and location, operating system and platform, device IDs, device type, mobile network information, app version number.
- **Transaction data:** your bank account and/or payment card details, details about payments to and from you and details of products and services you have purchased from us.



You must provide this personal data to use our website, app and/or hotel or club services, as relevant, unless we tell you that you have a choice.

Where you do have a choice, we will also tell you whether declining to share that personal data will have any effect on your use of our website, app and/or hotel or club services.

4. Lawful basis

UK and EU data protection law requires us to have a lawful basis for processing your personal data.

We rely on one or more of the following lawful bases:

- **Consent:** where we have obtained your active agreement to use your personal data for a specified purpose.
- **Performance of a contract:** where our processing is necessary to perform a contract we are about to enter into or have entered into with you.
- **Legal obligation:** where our processing is necessary for compliance with a legal obligation that we are subject to.
- **Vital interests:** in emergency situations when processing is necessary for your vital interests or those of another person.
- **Public task:** where processing is necessary for performance of a task carried out in the public interest.
- **Legitimate interests:** where processing is necessary to pursue our legitimate interests or those of a third party. We make sure we consider and balance any potential impact on you and your rights (both positive and negative) before we process your personal data for legitimate interests.
- **Legally recognised legitimate interests:** in some cases where UK law applies, we may process your personal data where this is necessary for specific legitimate interests that are recognised in law and based on public interests. These legitimate interests are as follows:
 - Public task disclosure requests: where it is necessary for us to share your personal data with a third party (on request by the third party) because they need it for purposes that are in the public interest or for a task carried out in the exercise of official authority, and set out in law. In practice, this will apply where we share your personal data with a public authority, or organisation, because they have sent us a request, which says that disclosure is needed for these purposes.
 - National security, public security and defence: where our processing of your personal data is necessary: (a) for the purposes of safeguarding national security, (b) for the purposes of protecting public security, or (c) for defence purposes. In practice, this will apply (particularly part (b)) when we need to process your personal data to protect our organisation, website, app, hotels, clubs, systems and assets against public threats, including crime, disasters and other risks to life, safety and well-being.
 - Emergencies: where our processing of your personal data is necessary for the purposes of responding to certain types of emergencies, which could include extreme weather events, pandemics or cyber-attacks on infrastructure.



- *Detecting, investigating and preventing crime*: where our processing of your personal data is necessary for the purpose of (a) detecting, investigating or preventing crime, or (b) apprehending or prosecuting offenders. This includes where we need to process your personal data to detect, investigate or prevent crimes like money laundering, terrorist financing, fraud, and/or social engineering (and scams).
- *Safeguarding vulnerable individuals*: where our processing of your personal data is necessary for the purposes of safeguarding a vulnerable individual (being (a) a child under the age of 18, or (b) an adult who is at risk).

More information about when we rely on all of the above lawful bases is set out in the sections below.

5. How we use your personal data

We use your personal data for the following purposes and on the following lawful bases:

The personal data marked (*) is required to be provided under the terms of our contracts and/or to enter into a contract for the purposes stated. If you cannot provide this data we may not be able to contract with you, and this may limit the services we can provide to you.

Purpose	Types of data (as reasonably necessary in the circumstances)	Lawful basis
To provide access to and maintain our website and app	(a) Location Data (b) Membership Data (c) Technical Data	Legitimate interests (<i>our legitimate interests in effectively running our website and app</i>) Consent (<i>to process Location Data via our app</i>)
To make and manage bookings	(a) Booking Data* (b) Communication Data (c) Contact Data* (d) Health Data (e) Identity Data* (f) Membership Data (g) Transaction Data*	Performance of a contract (<i>in particular, making amending and cancelling bookings and processing associated payments</i>) Legitimate interests (<i>our legitimate interests in managing your booking, including to take account of your preferences and/or requirements e.g. specific room preferences and/or dietary preferences or allergies</i>)

æthos

To check you in at one of our hotels or clubs and manage your stay	(a) Booking Data* (b) Contact Data (c) Health Data (d) Identity Data (e) Membership Data	Performance of a contract (<i>honouring your booking</i>) Legitimate interests (<i>our legitimate interests in managing your stay, including to take account of your preferences and/or requirements e.g. specific room preferences and/or dietary preferences or allergies</i>)
To register you as a member and manage your membership	(a) Booking Data* (b) Contact Data* (c) Membership Data* (d) Transaction Data*	Legitimate interests (<i>our legitimate interests in setting up memberships of our Aethos Members' Club on request, and providing benefits and experiences to registered members</i>)
To consider any job application that you submit through our website or app	(a) Candidate Data (b) Contact Data	Legitimate interests (<i>our legitimate interests in operating our business with suitably qualified staff</i>)
To process e-gift card purchases	(a) Contact Data* (b) Transaction Data*	Performance of a contract
To communicate with you (except where we send you marketing – see below)	(a) Booking Data (b) Candidate Data (c) Communication Data (d) Contact Data (e) Identity Data (f) Membership Data (g) Technical Data (h) Transaction Data	Legitimate interests (<i>our legitimate interests in effectively responding to and resolving communications, complaints and/or queries and to send to you service messages e.g. related to changes to this notice or website/app downtime</i>)
To send you marketing, including our newsletter	(a) Booking Data (b) Contact Data (c) Membership Data (d) Marketing Data	Legitimate interests (<i>our legitimate interests in supporting the growth and commercial success of our</i>

æthos

		<i>business through marketing by telephone or post)</i> Consent (<i>marketing by email and other electronic means and/or where using cookies and similar technologies</i>)
To undertake marketing initiatives, including allowing you to refer others to our membership program	(a) Booking Data (b) Contact Data (c) Membership Data (d) Marketing Data	Consent (<i>where required by law</i>) Legitimate interests (<i>our legitimate interests in supporting the growth and commercial success of our business through marketing initiatives, where applicable law does not require us to obtain your consent</i>)
To improve our website and app and personalise these services for users (including aggregating personal data so that it can subsequently be used on an anonymous basis for these purposes)	(a) Technical Data	Legitimate interests (<i>our legitimate interests in improving our website and/or app</i>) Consent (<i>where we use cookies or similar technologies for these purposes and consent is required by law</i>)
To protect our website, app, hotels, clubs, business, guests, staff and users, against: • security threats • emergencies • crime	(a) Booking Data (b) Candidate Data (c) Communication Data (d) Contact Data (e) Health Data (f) Identity Data (g) Location Data (h) Marketing Data (i) Membership Data (j) Technical Data (k) Transaction Data	Legally recognised legitimate interests (<i>relating to: (i) national security, public security and defence; and/or (ii) emergencies; and/or (iii) detecting, investigating and preventing crime (as described in more detail in section 4. above)</i>) Legitimate interests (<i>our legitimate interests in protecting our business and those individuals who interact with our business</i>) Legal obligation (<i>where we are legally required to take</i>

æthos

	We also use image and video data collected via CCTV for these purposes, where CCTV is installed at our hotels or clubs.	<i>certain action for these purposes)</i>
To obtain professional advice (e.g. legal advice)	(a) Booking Data (b) Candidate Data (c) Communication Data (d) Contact Data (e) Health Data (f) Identity Data (g) Location Data (h) Marketing Data (i) Membership Data (j) Technical Data (k) Transaction Data	Legitimate interests (<i>to help ensure the proper operation of our business and to defend our rights, interests, people and assets</i>)
To comply with our legal and regulatory obligations (where underpinned by law), such as those relating to tax, health and safety, competition law and data security, as well as complying with any court orders that are applicable to us	(a) Booking Data (b) Candidate Data (c) Communication Data (d) Contact Data (e) Health Data (f) Identity Data (g) Location Data (h) Marketing Data (i) Membership Data (j) Technical Data (k) Transaction Data	Legal obligation
To handle medical emergencies and manage medical conditions	(a) Booking Data (b) Contact Data (c) Health Data	Legally recognised legitimate interests (<i>relating to safeguarding vulnerable individuals, as described in more detail in section 4. above</i>) Vital interests

æthos

		Legitimate interests (<i>our legitimate interests in keeping guests and visitors safe whilst they are at our hotels or clubs</i>)
--	--	--

Opting out of marketing:

You can ask us to stop sending you marketing communications at any time by following the opt-out links within any marketing communication sent to you or by contacting us at hello@aethos.com.

If you opt out of receiving marketing communications, you will still receive service-related communications that are essential for administrative or customer service purposes.

Automated decision-making:

We do not make any significant decisions about you based solely on the automated processing of personal data without meaningful human involvement. We will notify you if this position changes.

Withdrawing consent:

Where you have provided your consent to our processing of your personal data, you can withdraw this at any time by contacting us at hello@aethos.com.

6. Who we share your personal data with

We share your personal data (described in section 3. above) where it is reasonably necessary to do so, as set out below:

- **Other Aethos group entities:** (see section 1. above): for the purposes of considering job applications, handling bookings and operating shared customer relationship management systems.
- **Tiquo Ltd:** this is our service provider, which provides us with customer relationship management ('CRM'), booking and payment functionality. Tiquo Ltd also engages subprocessors for these purposes. Its subprocessor list can be found [here](#) and may be updated from time to time.



- **Public authorities, regulators or other bodies exercising official functions:** in response to legitimate written requests from these entities.
- **Our advisers:** such as insurers, accountants, lawyers, tax advisors, where we require professional advice in relation to any of our activities.
- **Third parties that will or may take control or ownership of some or all of our business:** in connection with a significant corporate transaction or restructuring, including a merger, acquisition, asset sale, initial public offering or in the event of our insolvency.
- **Those we are legally required to share personal data with:** which includes law enforcement agencies, courts, tribunals, regulatory bodies and third parties who we are required to share personal data with under a court order.

7. Cookies (and similar technologies)

We use cookies and similar technologies that store information, and/or access information stored, on your 'terminal equipment' (e.g. a mobile phone or computer that you use).

For further information on:

- how we use these technologies;
- when and how we request your consent before using them; and
- how to disable them,

please see our [Cookie Policy](#)

8. International data transfers

We transfer your personal data outside the UK or the European Economic Area, or Switzerland (as applicable) in certain limited circumstances as explained below, or where a specific exception applies under relevant data protection law. However, we do not routinely rely on exceptions in respect of overseas transfers of personal data.

Transfers of personal data from the UK

- **Transfers under adequacy regulations:** we may transfer your personal data outside of the UK, where the UK government has decided that the country that the personal data will be transferred to ensure an adequate level of protection of personal data (by issuing 'adequacy regulations').

A list of countries the UK currently has adequacy regulations in relation to is available [here](#). This includes all countries in the EU.

We rely on adequacy regulations for transfers of personal data to our providers and group companies that are based in these countries, which includes:

- our group companies located in the EU (see section 1. for details); and
 - Aethos AG.
- **Transfers subject to contractual safeguards:** we may transfer your personal data outside of the UK in cases where there are 'appropriate safeguards' in place, such as standard data protection clauses approved under UK law, provided that the level of protection for your



personal data following the transfer will not be materially lower than in the UK. We do not currently conduct any transfers on this basis.

Transfers of personal data from the European Economic Area

- **Transfers under adequacy decisions:** we may transfer your personal data outside of the European Economic Area where the European Commission has decided that the country that the personal data will be transferred to ensures an adequate level of protection for personal data (by issuing an 'adequacy decision').

A list of current adequacy decisions made by the European Commission is available [here](#). This includes the UK. We rely on adequacy decisions for transfers of your personal data to our providers and group companies that are based in these countries. This includes:

- Aethos AG; and
 - Tiquo Ltd - our CRM, booking and payment provider (which is UK-registered).
- **Transfers subject to contractual safeguards:** we may transfer your personal data outside of the European Economic Area in cases where there are 'appropriate safeguards' in place, such as standard data protection clauses approved under EU law, provided that the level of protection for your personal data following the transfer is essentially equivalent to that in the European Economic Area. We do not currently conduct any transfers on this basis.

Transfers of personal data from Switzerland

Your personal data may be transferred to our group companies located in the EU (see section 1. for details) and Tiquo Ltd - our CRM, booking and payment provider (which is UK-registered).

Transfers of personal data by our providers

Our providers may also transfer your personal data outside of the European Economic Area, Switzerland or the UK (as applicable) when providing services to us. Tiquo Ltd - our CRM, booking and payment provider, uses subprocessors outside of the European Economic Area, Switzerland and the UK, including in the US. Further details, including information on the safeguards that it implements before making these transfers, are set out [here](#).

9. Retaining personal data

We will retain your personal data for as long as reasonably necessary to fulfil the purposes we collected it for and for the purposes of satisfying any legal, regulatory, tax, accounting or reporting requirements.

In practice, this means that we typically keep basic information about our customers after they cease being customers for a time period of between 6 and 10 years, depending on which country's laws apply.

We may also retain your personal data for a longer period in the event of a complaint or if we reasonably believe there is a prospect of litigation in respect to our relationship with you.

To determine the appropriate retention period for personal data, we consider:

- our contractual obligations and rights in relation to the personal data involved;
- the amount, nature and sensitivity of the personal data;
- the potential risk of harm from unauthorised use or disclosure of your personal data;



- applicable legal, regulatory, tax, accounting or other requirements that may require us to retain data for a certain period of time;
- any actual or potential disputes (including litigation) relating to that data; and
- guidelines on the retention of data, issued by relevant data protection authorities.

10. Your rights

You have certain rights under UK, Swiss and/or EU data protection law (as applicable) which are described below. These rights are subject to some limitations, and they are impacted by the lawful basis that we rely on for our processing of your personal data, and the availability of exemptions.

You will not have to pay a fee to access your personal data (or to exercise any of the other rights). However, we may charge a reasonable fee if your request is clearly unfounded, repetitive or excessive. Alternatively, we could refuse to comply with your request in these circumstances.

- **Right of access** - you have the right to ask us for copies of your personal data and certain other information similar to that provided in this privacy notice.
- **Right to rectification** - you have the right to ask us to correct personal data that you think is inaccurate or incomplete.
- **Right to erasure** - you have the right to ask us to delete your personal data.
- **Right to restriction of processing** - you have the right to ask us to limit how we can use your personal data.
- **Right to object to processing** - you have the right to object to the processing of your personal data.
- **Right to data portability** - you have the right, in certain circumstances, to ask that we transfer the personal data you gave us to another organisation, or to you.
- **Right to withdraw consent** - when we use consent as our lawful basis you have the right to withdraw your consent at any time.

If you would like to exercise your data protection rights or make a data protection complaint, you can submit your request or complaint to hello@aethos.com.

When we receive a data protection complaint that we have not complied with the UK GDPR, we will:

- Acknowledge receipt no later than 30 days from receiving it.
- Take appropriate steps to respond without undue delay, which will include:
 - making enquiries into the subject matter of the complaint (to the extent appropriate); and
 - keeping you informed about our progress in handling the complaint.
- Inform you of the outcome without undue delay.

When you make a request to exercise any of the rights referenced above, we may need to request specific information from you to help us confirm your identity. This is a security measure to ensure that personal data is not shared with any person who has no right to receive it.



We may also contact you to ask you for further information in relation to your request.

11. Changes to this Privacy Policy

We may change this Privacy Policy from time to time. When we make significant changes we will take steps to inform you, e.g. by including a prominent link to a description of those changes on our website and app (for a reasonable period) or by other means, such as email.

12. Contact us

If you have any questions about this Privacy Policy, please contact us at hello@aethos.com.

13. Contact the data protection regulator

If you have a complaint about our practices or a concern about this Privacy Policy, you may contact the relevant data protection regulator.

- In the UK this is:
 - the Information Commissioner's Office (and/or its successor organisation, the Information Commission) at: <https://ico.org.uk/make-a-complaint/>
 - The ICO's address is: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF.
- In the EU, a list of regulators and their contact details are set out [here](#).
- The Swiss data protection regulator can be contacted [here](#).