

Privacy Notice for Harmony Pilates

1. Data Controller and Contact Details

Data Controller: Harmony Pilates (the “Studio”) – Derendorfer Straße 76, 40479 Düsseldorf, Germany.

Contact: info@harmonypilates.de | 01786283389

The Studio is responsible for deciding how and why your personal data are processed (data controller). If you have any questions or concerns about your personal data, please contact us at the details above.

2. Personal Data We Collect

We collect only the personal information necessary to provide our services. This includes:

- **Identity and Contact Details:** Name and surname, email address, telephone number, and (if provided) postal address. We also collect your date of birth to ensure you are an adult (minors under 18 cannot sign up).
- **Health Information:** Relevant medical details you choose to provide (e.g. injury history, pregnancy status, scoliosis or other health conditions) that are needed for your safe participation in our classes. This health data is considered *special category* personal data under GDPR.
- **Booking and Membership Data:** Class bookings, attendance records, membership package details, and any communications or preferences (e.g. class waitlists or schedule changes).
- **Payment Information:** When you make purchases (such as class packages), payment details are processed securely via our booking platform Bsport or its integrated payment provider (e.g. Stripe). We **do not** store your full credit card details on our systems.

No Data from Minors: Our services are intended for adults. We do not knowingly collect personal data from anyone under 18 years of age. If we learn that a minor has provided us personal information, we will delete it.

3. Purposes and Legal Bases for Processing

We process your personal data **only for legitimate purposes and in accordance with the GDPR’s legal bases:**

- **Service Provision (Booking and Classes):** To create and manage your Studio account, schedule classes, process payments, and provide you with Pilates instruction. This is **necessary for the performance of our contract** with you (Art. 6(1)(b) GDPR) – for example, we need to use your name and contact info to register you and send class confirmations. Health information you provide is used to tailor our services to you (e.g. modifying exercises for an injury) and ensure your safety. Because health data is sensitive, we rely on your **explicit consent** (Art. 9(2)(a) GDPR) to process that

information. You may withdraw this consent at any time (though doing so may limit our ability to safely include you in certain classes).

- **Communications and Customer Support:** To communicate with you about class schedules, cancellations, instructor changes, or respond to your inquiries. These communications are part of our service (contractual necessity, Art. 6(1)(b)) and/or our legitimate interest in providing good customer service (Art. 6(1)(f) GDPR).
- **Marketing to Current Clients: Limited marketing** is sent to keep our current members informed about studio news, new classes or promotions. We rely on our **legitimate interests** (Art. 6(1)(f) GDPR) for this purpose, as GDPR acknowledges that direct marketing to existing customers may be a legitimate interest. We only send such marketing to those who are currently clients or members, and **never sell or share your data with third parties for their own marketing**. You have the right to object to or opt out of our marketing at any time (see **Marketing and Opt-Out** below).
- **Legal Obligations:** To comply with laws and regulations, such as retaining transaction records for tax/audit (Art. 6(1)(c) GDPR). For instance, we may keep invoice information as required by financial laws.
- **Safety and Fraud Prevention:** To protect our rights, your safety, and the security of our services (e.g. preventing fraud or misuse of our booking system). This is another legitimate interest (Art. 6(1)(f)) and, where applicable, a legal obligation.

We will not use your personal data for any purpose that is incompatible with the ones listed above. If we need to process your data for a new purpose, we will inform you and, if required, seek your consent.

4. Data Sharing and Recipients

We treat your personal data with care and **do not sell it** to third parties. We only share data as necessary to run our studio services, under strict agreements:

- **Bsport (Booking Platform):** We use Bsport as our online booking and membership management system. When you register and book classes through Bsport, your personal data is stored in Bsport's system. This includes your contact details, membership and booking history, and any health information you provided (from our pre-exercise questionnaire) so that instructors are aware of relevant health issues during classes. Bsport acts as our *data processor*, meaning they process your data on our behalf and under our instructions. Bsport is contractually obliged to protect your data and is GDPR-compliant. You can refer to Bsport's own Privacy Policy for more details on their data practices.
- **Payment Processor:** If you pay by credit card via Bsport, the payment is handled by Bsport's integrated payment provider (e.g. Stripe). Your card details are sent directly to the payment processor and are not stored by us. The payment processor will have its own privacy and security measures in line with GDPR.
- **Email and IT Service Providers:** We may use secure third-party services for emailing class reminders or newsletters (for example, if we integrate an email service or use Bsport's email features). Any such provider will only get the information needed to send the emails (typically your name and email) and must also comply with data protection law.

- **Legal or Compliance Recipients:** If required by law, we may disclose data to authorities or regulators. For example, if a law or court order compels us to provide information, or to enforce our legal rights or handle legal claims. We will only share the minimum necessary in such cases.

Aside from the above, our staff and instructors have access to your relevant personal data **only on a need-to-know basis** – for instance, instructors see your name on class rosters and any health notes you’ve given so they can teach you safely. All personnel are bound by confidentiality. We will **never share your data with third parties for their own marketing** or unrelated purposes, unless you have explicitly consented to such sharing.

5. Data Retention – How Long We Keep Your Data

We retain your personal data **only for as long as necessary** to fulfill the purposes outlined in this notice, and to satisfy legal, accounting, or reporting requirements. In practice:

- **Member Account and Class Records:** We keep your account information and class attendance records while you are an active client. If you stop using our services or your membership ends, we generally retain your data for a limited period before deletion. This allows us to meet any legal obligations or address any issues that arise after you leave.
- **Health Information:** Health and injury information you provide is kept as long as you are a client, and for a short period after in case you return or for safety record-keeping. If you withdraw your consent for us to hold this sensitive data, we will delete it (unless we need to keep it for legal reasons).
- **Payment and Transaction Data:** We retain transaction records (e.g. invoices, payment confirmations) for the duration required by tax and financial laws (in Germany, typically **10 years**). These records may include personal data like your name or contact on receipts, which we must keep by law.
- **Marketing Preferences:** If you opt out of marketing, we will keep a record of your opt-out (email address suppressed from mailing lists) to ensure we respect your choice in the future.
- **Website Logs:** Basic web server logs and analytics data are kept for a short period as needed for security and analysis, and are then anonymized or deleted.

After the applicable retention period, we will either securely delete your personal data or anonymize it (so it can no longer be linked to you). We will also do so sooner upon your verified request, provided no legal obligations prevent us from deletion. We **never retain your information longer than necessary** under GDPR principles.

6. How We Secure Your Data

Data security is very important to us. We implement appropriate technical and organizational measures to protect your personal data against unauthorized access, loss, or alteration. These measures include:

- **Encryption & Access Control:** We use secure systems to store data, with encryption and password protection where appropriate. Access to personal data is restricted to authorized

staff and service providers who need it to perform their duties. For example, our booking platform and databases are protected by authentication and encryption.

- **Secure Transmission:** When you enter sensitive information (like health details or payment info) on Bsport's platform, the transmission is encrypted via SSL/TLS. This means your data is securely sent over the internet.
- **Physical and Managerial Safeguards:** Any paper forms (such as health questionnaires, if used) are kept in a secure location. Our computers and devices are protected by firewalls and antivirus software, and we train our team on data protection best practices.
- **Regular Monitoring:** We regularly update our software and platforms to address security vulnerabilities. Bsport, as our processor, also adheres to high security standards and monitors its systems.

While we strive to protect your information, please note that **no method of transmission or storage is 100% secure**. However, we continually review and improve our security measures to meet or exceed industry standards and legal requirements (Art. 32 GDPR). If we ever experience a data breach that poses a risk to you, we will notify you and the authorities as required by law.

7. Your Rights as a Data Subject

Under the GDPR, you have several **rights regarding your personal data**. You can exercise these rights at any time by contacting us (see **Data Controller and Contact Details** above). Your rights include:

- **Right to Be Informed:** The right to receive clear information about how we process your data (fulfilled by this Privacy Notice).
- **Right of Access:** You can request a copy of the personal data we hold about you. This allows you to check what information we have and confirm that we are processing it lawfully. We will provide you with a copy of your data, typically within one month of your request (free of charge).
- **Right to Rectification:** If any of your personal data is inaccurate or incomplete, you have the right to have it corrected. For example, you can update your contact information or health details at any time.
- **Right to Erasure:** Also known as the "right to be forgotten," you can ask us to delete your personal data in certain circumstances. For instance, if you cancel your membership and want all personal details removed, or if you withdraw consent for us to use your health data, we will erase the data provided we don't have a legal obligation to keep it.
- **Right to Restrict Processing:** You can request that we limit how we use your data (e.g. store it but not use it) in certain cases. This might apply if you contest the accuracy of the data or have objected to processing (pending our review).
- **Right to Data Portability:** You have the right to receive your personal data in a commonly used, machine-readable format, and/or have us transmit it to another service provider at your request. For example, if you move to another studio that uses a different system, we can assist in transferring your basic data to them, upon your request.
- **Right to Object:** You may object to any processing of your data that we do based on legitimate interests. This includes the right to object to our marketing communications at any time. If you object, we will stop that processing unless we have compelling legitimate

grounds to continue (or if it's required by law). **If you object to direct marketing, we will always honor your request immediately.**

- **Right to Withdraw Consent:** Where we rely on your consent (e.g. for health information or optional marketing emails), you have the right to withdraw that consent at any time. Withdrawal of consent will not affect the lawfulness of processing already carried out, but it means we will stop the specific processing going forward. For example, you can remove or update your health details in your profile, or unsubscribe from our newsletter.
- **Right not to be subject to automated decisions:** We do not use automated decision-making or profiling in our studio. If that changes, you would have the right to not be subject to a decision based solely on automated processing that significantly affects you.

To exercise any of these rights, please contact us via the email provided. We may need to verify your identity for security purposes before fulfilling your request. We will respond to your request as soon as possible, typically within **one month** as required by GDPR. There is no fee for exercising your rights. If we cannot comply with your request (for example, if you ask us to delete data which we must keep by law), we will explain the reason and inform you of your options.

Lastly, you also have the **right to lodge a complaint** with your local Data Protection Authority if you believe we have processed your data unlawfully. In Germany, you can contact the North Rhine-Westphalia data protection authority (LDI NRW), or your respective supervisory authority, for guidance or to file a complaint. We would, however, appreciate the chance to address your concerns directly first.

8. Marketing Communications and Opt-Out

We value your privacy and will **not spam you** or send irrelevant marketing. Here is how we handle marketing communications:

- **Current Clients and Members:** As our client, we may send you occasional updates about our studio – for example, new class offerings, schedule changes, special offers or events. We send these communications based on our legitimate interest to keep our members informed about relevant services. **We do not send marketing messages to people who are not our clients** (unless they separately subscribe to a newsletter).
- **Opt-In for Newsletters:** At the time of registration, you may be asked if you want to receive our newsletter or promotional emails. This is voluntary. If you opt in (or sign up for our newsletter on our website), we will use your email to send you studio news. If you choose not to opt in, we will only send you essential service-related emails (e.g. booking confirmations or class cancellations).
- **How to Unsubscribe:** Every marketing email we send will include an “unsubscribe” link at the bottom. You can click this link at any time to stop receiving further newsletters or promotions. You can also opt out by adjusting your preferences in your Bsport account profile or by contacting us directly. We will immediately honor your opt-out request and you will not receive future marketing emails. There is no penalty or effect on your ability to use our services if you choose to opt out.
- **No Third-Party Marketing:** We will not share your personal data with other companies for their marketing. You will only receive studio-related communications from us.

Please note that even if you opt out of marketing, we may still send you **transactional or service messages** (such as booking confirmations, class reminders, or important notices about your membership) as these are not promotional, but necessary for our contract with you.

9. Data Sharing with Bsport – Additional Note

(This section is for transparency regarding our booking platform Bsport, as it plays a key role in processing your data.) Bsport is a third-party platform that **hosts our class schedule, bookings, and member database**. In most cases, the personal data you provide to us is entered into the Bsport system. The Studio remains the data controller, and Bsport acts as a data processor on our behalf. Bsport's obligations to protect your data are outlined in our agreement with them, and they too must comply with GDPR. If you are using Bsport (via our website integration or the Bsport app) to manage your bookings, **please also review Bsport's Privacy Policy** for information on how Bsport handles data (e.g. cookies on their site, technical security, etc.). If you have any questions about data in the Bsport system, you can contact us or Bsport directly. We work closely with Bsport to resolve any data protection issues that might arise.

11. Updates to this Privacy Notice

We may update this Privacy Notice from time to time to reflect changes in our practices or for other operational, legal, or regulatory reasons. When we make changes, we will update the “last updated” date and, if the changes are significant, we may inform you directly (for example, via email or a notice on our website). We encourage you to review this notice periodically to stay informed about how we protect your personal data.

Last Updated: 09.08.2026.

By using our services or website, you acknowledge that you have read and understood this Privacy Notice. We are committed to protecting your personal data and respecting your privacy rights. If you have any questions or concerns about this notice or your personal data, please do not hesitate to contact us.