Privacy Policy (GDPR)

Privacy statement for the Apptimate Academy course platform

Document	Privacy Policy (GDPR)
Service	Apptimate Academy (online course platform)
Provider	Apptimate B.V. (KvK-nummer 89656202)
Version	1.0 (concept)
Effective date	[to be set]

Apptimate B.V. processes personal data in accordance with the General Data Protection Regulation (GDPR). This statement explains which data we process when you use the course platform, and why.

1. Data Controller

- Controller: Apptimate B.V. (KvK-nummer 89656202)
- Address: Postbus 2039, 1990 AA Velserbroek, Nederland
- Privacy contact: academy@apptimate.nl

2. What Data We Process

In connection with your account, your purchases, and your progress, we process the following categories of personal data:

- Name and email address (for your account and communication);
- Password: only as an encrypted hash (we never store your password in readable form);
- Preferred language;
- Account and consent data: the date your account was created and the time you accepted our terms;
- Purchase data: which course or bundle, amount, status, and a payment reference, with date;
- Progress data: which lessons you have completed and when, and when you first viewed a (free) lesson;
- Certificate data: the name shown on your certificate, a unique certificate code, and the date of issue;
- Data about reminder emails sent (whether and when a reminder was sent, and whether you unsubscribed);
- Session data: for each active login we store a hashed reference to your session, a truncated IP address (the network part only, not your full address), a hashed representation of your browser characteristics, and the time of sign-in and last activity. We use these solely to monitor how many devices are signed in to one account at the same time;
- Data about failed attempts: to counter automated guessing we briefly count failed sign-in attempts, password-recovery requests and attempts to change your password. We store no readable e-mail address and no full IP address for this, only a hashed representation of them with a counter and a timestamp;
- Password-recovery data: if you request a new password we store a hashed representation of the recovery code, the time of the request and the time it was used. The code itself only exists in the e-mail you receive;
- Contact-form data: your name, e-mail address, optionally your organisation, and the content of your message. We receive these as an e-mail and use them solely to answer your question; we do not store the message in the website;

- Technical data: your IP address and browser data (User-Agent) may appear in server logs for security and abuse prevention.

3. Data We Do NOT Store

- Credit card data or other payment data;
- Your password in readable (non-hashed) form.

Payments are processed by the payment provider 2CO. Payment data is processed by that service; only your name, email address, and a payment reference reach us.

4. Purposes and Legal Bases

- Creating and managing your account and providing access to purchased courses — basis: performance of the contract.
- Tracking your progress and issuing certificates — basis: performance of the contract.
- Processing payments and administration — basis: performance of the contract and legal obligation (tax retention).
- Reminder emails after a free preview lesson — basis: legitimate interest (informing you about a course you viewed), with the ability to unsubscribe at any time.
- Security, logging, and abuse prevention — basis: legitimate interest in the security and integrity of the service.
- Limiting the number of devices signed in to one account at the same time, in order to counter account sharing — basis: legitimate interest in preventing unlawful use of paid course content, and performance of the contract (your account is personal and non-transferable). We process as little data as possible for this: no full IP address and no readable browser data. We never block on an automated signal alone; a decision to block or terminate an account is always taken by a member of staff.
- Limiting the number of failed sign-in, recovery and password-change attempts — basis: legitimate interest in protecting your account against automated password guessing. We never count on e-mail address alone, so nobody can deliberately lock you out of your own account.
- Setting a new password after you have forgotten yours — basis: performance of the contract (access to your account).
- Answering questions you send through the contact form — basis: legitimate interest in responding to (prospective) customers, and where it concerns a quotation or an order: taking steps at your request prior to entering into a contract.
- Customer communication and support — basis: performance of the contract.

5. Retention Periods

- Account, progress, and certificate data: retained while your account exists. On an erasure request we delete them, except data we are legally required to keep.
- Purchase and payment records: we retain records subject to tax retention obligations for seven (7) years.
- Reminder-email data: retained as long as needed to prevent duplicate emails, then deleted.
- Session data: deleted as soon as you sign out, as soon as the session is replaced by a newer sign-in, and in any event no later than thirty (30) days after the last activity in that session. In practice this happens within a few hours.
- Data about failed attempts: deleted once the relevant period has passed, at the latest within a few hours of the last attempt.

- Password-recovery data: a recovery code is valid for sixty (60) minutes and can be used once; the data is deleted afterwards.
- Contact-form messages: kept in our mailbox for as long as needed to handle your question and, where it concerns a quotation or an order, for as long as our records require.
- Server logs (with IP/User-Agent): retained for a limited period for security purposes and then deleted or rotated.

6. Recipients and Transfers

We share data only with service providers necessary for our operations, such as the payment provider 2CO, our email/SMTP provider, and our hosting provider. We conclude data processing agreements with processors. Where data is processed outside the EEA, we apply appropriate safeguards, such as the European Commission's standard contractual clauses.

7. Your Rights

You have the right of access, rectification, erasure, restriction, objection, and data portability. Requests may be directed to academy@apptimate.nl. On an erasure request we delete your account, progress, and certificate data, except where retention is legally required (such as tax retention for purchases). You also have the right to lodge a complaint with the Dutch Data Protection Authority (Autoriteit Persoonsgegevens).

You may object to processing we base on a legitimate interest, including the monitoring of how many devices are signed in at the same time. We will weigh your objection against our interest in countering account sharing and inform you of the outcome with reasons.

8. Security

We take appropriate technical and organizational measures to protect personal data. Passwords are stored as a strong hash; traffic runs over HTTPS; database access uses parameterized queries; access to administrative functions is restricted; repeated failed sign-in attempts are slowed down. Vulnerabilities may be reported via security@apptimate.nl (see the Security Policy).

9. Changes

We may amend this privacy statement. The current version is available at apptimate.academy.