

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	1.1
Effective date	30 August 2026

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)
- Postal address: Postbus 2039, 1990 AA Velserbroek, Nederland
- Registered office: Floraronde 247, 1991 LA 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;
- Consent data for a purchase: which declarations you accepted before checkout, in which version and language, at what time, under which order number, and the moment access was granted;
- Licence data for a team licence: the licence codes, the work email address the buyer assigned to a seat, the moment the invitation was sent, and whether and when a code was redeemed (see section 7);
- 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.

About IP addresses, to avoid a misunderstanding: your full IP address appears in the web server logs, as it does on almost every website. Within the platform itself — for your sessions and for failed attempts — we deliberately do not record a full IP address, only a shortened or hashed representation.

3. Payment Data and What We Do Not Store

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

Payments through the Platform 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.

For as long as we sell on invoice only, that route is not used and your data does not reach the payment provider 2CO. If we reopen checkout through the Platform, the previous paragraph applies again and we will say so in this statement.

Where a business customer purchases on invoice, we invoice them ourselves. For that purpose we process the company and contact details the customer provides: company name, registered and billing address, VAT identification number, Chamber of Commerce number, the name and email address of the contact person, and any purchase order number. The legal bases are the performance of the agreement and our statutory obligation to issue and retain invoices; the retention period is seven years. See the Business Terms.

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.
- Making an issued certificate publicly verifiable, so that a third party to whom you show it can check its authenticity — basis: performance of the contract. The verification page shows only the certificate code, the validity status, the name of the course, and the date of issue; your name is not shown there.
- Processing payments and administration — basis: performance of the contract and legal obligation (tax retention).
- Recording your consent to immediate delivery and the loss of the right of withdrawal — basis: legal obligation and performance of the contract; we must be able to demonstrate what you accepted. This arises only on a purchase by a consumer through the Platform. On a business purchase there is no right of withdrawal to waive and these fields stay empty.
- Sending invitations containing a licence code and administering the seats within a team licence — in doing so we act on the employer's instructions and are a processor; the employer, as controller, determines the legal basis. Once the employee redeems their code and obtains an account, we are an independent controller for everything that follows. See section 7.

- Reminder emails after a free preview lesson, pointing you to the course you viewed and to the option of taking it for your team — basis: your consent, given in advance through a box that is never pre-ticked and that you may leave empty. You can withdraw that consent at any time through the unsubscribe link in every mail; withdrawal works for the future and has no effect on your account or your courses. We send this mail only if you gave that consent and were signed in when you viewed the preview lesson; a visitor who is not signed in is not recorded.
- 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.
- Following up on a quotation you requested that has not yet been accepted — basis: taking steps at your request prior to entering into a contract. We send at most one reminder for this, and only while the quotation is still valid.
- 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, including the consent data for that purchase: we retain records subject to tax retention obligations for seven (7) years.
- Licence data for a team licence: retained for as long as the licence runs and afterwards as part of the purchase records. We delete an assigned email address at the request of the person concerned or of the buyer, unless it belongs to a redeemed seat we must be able to account for administratively.
- Your consent for reminder emails and its withdrawal: retained for as long as we must be able to show that we were allowed to mail you, and for no longer than twenty-four (24) months after you withdrew it.
- Reminder-email data (which reminder was sent for which account and when): retained for up to twenty-four (24) months after sending and deleted thereafter. For as long as we keep them, they prevent you from receiving the same reminder twice.
- 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 up to twenty-four (24) months after your question has been dealt with. Where the message forms part of a quotation, an order, or a dispute, the retention period of the records it belongs to applies.
- Server logs (with IP/User-Agent): retained for up to ninety (90) days and rotated or deleted thereafter. Where longer retention is necessary to investigate a security incident or misuse, we retain only what that investigation requires, and no longer than it requires.

6. Cookies

We place functional cookies only: a session cookie to keep you signed in, and storage for your language choice and for protecting forms against misuse. No consent is required for these, as they are necessary for a service you requested yourself. We place no analytical, advertising, or tracking cookies. The full overview is in our Cookie Policy; that document governs on this point, so that two places do not have to say the same thing.

7. Recipients and Transfers

We share data only with service providers necessary for our operations. At present these are Strato (Germany) for hosting the platform and storing the database, and Strato (Germany) for sending our email. Both process within the European Economic Area, so these processing activities involve no transfer to a third country.

If checkout through the Platform is reopened, the payment provider 2CO joins them as a recipient; see chapter 3. We may also provide data to our accountant or to a competent authority where the law requires it. We do not sell your data and do not use it for advertising.

We conclude data processing agreements with processors. Should processing nevertheless take place outside the EEA, we apply appropriate safeguards, such as an adequacy decision or the European Commission's standard contractual clauses, and we state that here.

8. Team Licences: Email Addresses Supplied by the Employer

Where an employer buys a team licence, they may enter the work email address of an employee for each seat. At their request we send that address an invitation containing the licence code, and we keep the address with the licence so the employer can administer it. At that moment the employee has no account with us and did not supply the address themselves; we therefore inform them about this processing and about this statement at the latest in that invitation.

Legal basis: in this phase the employer is the controller and determines the legal basis; we process the address solely on their instructions and do not put forward a legal basis of our own. We process no more than the email address, the moment of invitation, and the status of the code.

Roles, in two phases. Before redemption the employer is the controller and we are a processor: we send the invitation and report back the licence status on their instructions, and the data processing provisions in the Business Terms apply to that. After redemption we are an independent controller for the employee's account, their progress, their certificates, and our support; the employee is then our own user. We therefore do not hold both roles at once for the same processing.

What the employer sees: only which address they assigned to a seat and whether that code has been redeemed, with the date. This is needed to know which seats are still free and who still needs a reminder. What the employer does not see: which lessons have been completed, how far anyone has progressed, which certificates have been obtained, and what the employee discusses with our support. We do not share those data with the employer.

If you are the employee and do not want your address kept with the licence, or wish to object to this

processing, you can tell us via academy@apptimate.nl. We will then delete the address, unless the seat has already been redeemed and we must be able to account for that purchase administratively.

9. 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). A certificate already issued remains valid, but we switch off its public verification. You also have the right to lodge a complaint with the Dutch Data Protection Authority (Autoriteit Persoonsgegevens), PO Box 93374, 2509 AJ The Hague.

We respond within one month of receiving your request. Where a request is complex we may extend that period by no more than two months, and we will tell you so within the first month. To avoid providing data to the wrong person, we may ask you to send your request from the email address of your account, or to make it plausible in another way that you are the person concerned. Handling your request is free of charge.

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. Where it concerns the email address your employer entered for a team licence, the employer is the controller for that; you may address them and may also tell us, see section 7.

10. Automated Decision-Making and Profiling

We do not take decisions with legal or similarly significant effects for you that are based solely on automated processing, and we do not build profiles to predict your behaviour or your characteristics.

Our systems do produce automated signals: for example when more devices are signed in to one account than permitted, or when there is an unusual number of failed sign-in attempts. Such a signal may lead to a short delay or to ending the least recently used session. A decision to block or terminate an account, however, is always taken by us after review by a member of staff, and never on such a signal alone. If you disagree with such a decision, tell us via academy@apptimate.nl.

11. Minors

Our service is aimed at adults learning professionally and is not intended for children. To create an account independently you must be at least 18 years of age; see the Terms of Service. If we find that we have processed a minor's data without the required consent, we delete it as soon as possible. If you believe this is the case, tell us via academy@apptimate.nl.

12. 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).

If a breach nevertheless occurs that poses a risk to your rights and freedoms, we report it within seventy-two (72) hours to the Dutch Data Protection Authority and, where the law requires it, to you as well.

13. Changes

We may amend this privacy statement, for instance when we engage a new service provider or add a feature. The current version is always available at apptimate.academy, with the version number and date at the top. For a significant change — a new purpose or a new category of recipients — we inform holders of an active account by email before the change takes effect.