Privacy Policy (GDPR)

1. About this Policy

This Privacy Policy explains how Vidda Solutions AS ("Vidda", "we", "us", or "our") collects, uses, shares, and protects personal data when you visit our website, register an account on the Vidda HUB platform (the "Platform"), purchase or access training content, or otherwise interact with us.

This Policy is incorporated into and forms part of the Vidda HUB Buyer Terms of Use. Capitalised terms used but not defined in this Policy have the meanings given to them in the Buyer Terms of Use or, where applicable, in Annex A — Buyer Data Processing Agreement.

2. Who we are

Vidda Solutions AS is a private limited company registered in Norway with organisation number 834 081 652.

For privacy-related enquiries you may contact us at:

- **Email:** support@vidda.io

Inndeling 1.01 **Post:** Vidda Solutions AS, Ostadalsveien 3 A, 0753 Oslo, Norway

We have not formally appointed a Data Protection Officer ("DPO") as we are not legally required to do so under GDPR Article 37. Georg Muri, Chief Product Officer serves as our internal privacy point of contact.

3. Scope of this Policy and our role

This Policy applies to personal data we process about:

- **Individual Buyers** — natural persons who purchase access to Content for personal use;
- **Corporate Buyer administrators** — individuals who register, manage, or operate a Corporate Buyer account on behalf of an organisation;
- **Content Providers and their personnel** — individuals associated with third parties that supply Content to the Platform;
- **Website visitors** — individuals who visit vidda.io or interact with our public-facing materials;
- **Prospective customers and business contacts** — individuals we communicate with for sales, marketing, or partnership purposes.

In relation to all of the above categories, Vidda acts as a Data Controller.

Inndeling 1.02 Important — Learner personal data

Where a Corporate Buyer enrols Learners (employees, contractors, or other authorised individuals) on the Platform, Vidda processes those Learners' personal data on behalf of the Corporate Buyer. In that context, the Corporate Buyer is the Data Controller and Vidda is the Data Processor.

The processing of Learner personal data is governed by Annex A — Buyer Data Processing Agreement, not by this Privacy Policy. Learners should consult the privacy notice provided by their employer or contracting organisation for information about how their personal data is processed.

4. Personal data we collect

The categories of personal data we collect depend on how you interact with us.

Inndeling 1.03 4.1 Account and purchase data

- Full name
- Email address (work or personal)
- Job title and organisation name (where provided)
- Country of residence and billing address
- Payment-related information (processed by our payment provider — see section 8)
- Account credentials (stored in encrypted form)
- Purchase and transaction history
- Communication preferences

Inndeling 1.04 4.2 Platform usage data

- Login times and IP address
- Device, browser, and operating system information
- Content accessed and Completion Records generated under your account
- Interactions with Platform features (clicks, searches, navigation)

Inndeling 1.05 4.3 Communications data

- Records of correspondence with our support, sales, and account management teams
- Survey responses and feedback you choose to provide

Inndeling 1.06 4.4 Website and cookie data

Information collected via cookies and similar technologies. See section 13 for details.

We do not intentionally collect special categories of personal data (such as data revealing racial or ethnic origin, religious beliefs, health, or sexual orientation). Please do not submit such data to us through Platform forms or support channels.

5. How we use your personal data and our legal bases

GDPR requires us to have a legal basis for each processing activity. The table below sets out our main processing purposes and the legal bases we rely on.

Purpose	Categories of data	Legal basis (GDPR Art. 6)
Creating and managing your account and providing the Platform	Account data, credentials	Performance of a contract — Art. 6(1)(b)
Processing payments and issuing invoices	Account data, transaction data	Performance of a contract; legal obligation (tax / accounting) — Art. 6(1)(b), (c)
Granting and tracking Content access; generating Completion Records	Account data, Platform usage data	Performance of a contract — Art. 6(1)(b)
Providing customer support	Communications data, account data	Performance of a contract; legitimate interests — Art. 6(1)(b), (f)
Sending service notifications (e.g. access changes, security alerts)	Account data, email address	Performance of a contract; legitimate interests — Art. 6(1)(b), (f)
Marketing communications about Vidda products and services	Email, communication preferences	Consent or legitimate interests, depending on jurisdiction — Art. 6(1)(a) or (f)
Platform analytics and service improvement	Platform usage data, pseudonymised identifiers	Legitimate interests — Art. 6(1)(f)
Fraud prevention, security monitoring, and abuse detection	Account data, IP, usage logs	Legitimate interests; legal obligation — Art. 6(1)(f), (c)
Complying with legal obligations (tax, accounting, regulatory requests)	Account and transaction data	Legal obligation — Art. 6(1)(c)
Establishing, exercising, or defending legal claims	Any relevant data	Legitimate interests — Art. 6(1)(f)

Our legitimate interests include operating and securing the Platform, improving our services, growing our business, and protecting our rights and those of our users. Where we rely on

legitimate interests, we have balanced these against your rights and freedoms. You may object to processing based on legitimate interests at any time (see section 12).

Marketing. Where we send marketing communications based on consent, you may withdraw consent at any time using the unsubscribe link in our emails or by contacting us. Withdrawal does not affect the lawfulness of processing carried out before withdrawal.

6. When we act as a Processor (Learner data)

When a Corporate Buyer enrols Learners on the Platform, we process the following categories of Learner personal data on the Corporate Buyer's behalf and on its documented instructions:

- Full name and work email address
- Organisation name and (where provided) job title
- Course access logs, completion status, and assessment results
- Date and time of Platform access

This processing is governed by Annex A — Buyer Data Processing Agreement, which sets out the parties' respective obligations, the technical and organisational security measures applied, sub-processor arrangements, breach notification timelines, and data subject rights handling.

Learners exercising their data subject rights should generally direct their requests to their employer or contracting organisation, which is the Data Controller. Where we receive such requests directly, we will forward them to the relevant Corporate Buyer in accordance with the DPA.

7. Sources of personal data

Most of the personal data we hold about you is provided by you directly — when you register, make a purchase, contact our support team, or use the Platform.

We may also receive personal data from:

- **Your employer or contracting organisation** where you are enrolled as a Learner;
- **Our payment provider (Dintero)** in relation to transactions you make;
- **Third-party services integrated with the Platform** where you choose to use them;
- **Publicly available sources** (e.g. professional networking sites) for business contact and sales purposes, in accordance with the relevant platform's terms of use.

8. Sharing personal data and sub-processors

We do not sell your personal data. We share it only in the circumstances described below.

Inndeling 1.07 8.1 Service providers (sub-processors)

We engage trusted third parties to support the operation of the Platform. These providers act on our documented instructions and are bound by written data protection terms equivalent to those required by GDPR Article 28.

Sub-processor	Location	Purpose
Amazon Web Services (AWS)	Ireland (EEA)	Infrastructure and data hosting
Dintero	EEA	Payment processing
Amplitude	Frankfurt (EEA)	Platform usage analytics
Microsoft 365	EEA	Transactional email and business communications

The current list of sub-processors used in the processing of Learner data is also maintained in Schedule 1 to Annex A. We will update this list when sub-processors are added, replaced, or removed.

Inndeling 1.08 8.2 Content Providers

Where you access Content, we may share aggregated or anonymised usage information with the relevant Content Provider to help them improve their materials. Where necessary to operate the Platform or to deliver the access arrangements you have agreed to, limited personal data (such as completion status linked to your name) may be shared with a Content Provider.

Inndeling 1.09 8.3 Professional advisers

We may share personal data with our auditors, lawyers, accountants, and insurers where reasonably necessary, subject to confidentiality obligations.

Inndeling 1.10 8.4 Legal and regulatory disclosures

We may disclose personal data where required by law, by court order, or by a competent regulatory authority, or where necessary to establish, exercise, or defend legal claims.

Inndeling 1.11 8.5 Business transfers

If Vidda is involved in a merger, acquisition, financing, reorganisation, or sale of assets, personal data may be transferred as part of that transaction. The recipient will be required to protect personal data in a manner consistent with this Policy.

9. International data transfers

Vidda is based in Norway, and our primary infrastructure is located within the European Economic Area ("EEA"). We aim to keep personal data within the EEA wherever possible.

Where personal data is transferred outside the EEA — for example, where a sub-processor's support team is based in another country — we ensure that one of the following safeguards is in place:

- the destination country benefits from a European Commission adequacy decision; or
- Standard Contractual Clauses ("SCCs") adopted by the European Commission are in place; or
- another lawful transfer mechanism under GDPR Chapter V applies.

Where SCCs are relied on, we carry out a transfer impact assessment and apply supplementary measures (such as encryption) where appropriate. You may request a copy of the relevant safeguards by contacting us at the address in section 17.

10. How long we keep your personal data

We keep personal data only for as long as necessary for the purposes for which it was collected, including to satisfy any legal, accounting, or reporting requirements. After the applicable retention period, we securely delete or anonymise the data.

Category of data	Retention period
Account data	Duration of your account plus 12 months following closure
Transaction and invoicing data	Minimum 5 years after the relevant accounting year, as required by the Norwegian Bookkeeping Act
Completion Records	3 years from the date of the relevant activity, unless a longer period is requested in writing
Support and communications data	Up to 3 years after resolution of the relevant matter
Marketing data	Until you unsubscribe or object, followed by a short suppression-list retention to honour your opt-out
Website analytics data	Up to 14 months in identifiable form, then aggregated
System and security logs	Up to 12 months, unless required for longer for legal or security purposes
Backups	Standard backup cycle, typically not exceeding 90 days

11. How we protect your personal data

We have implemented appropriate technical and organisational measures designed to protect personal data against unauthorised access, alteration, disclosure, loss, or destruction. These measures include:

- Encryption of personal data in transit (TLS) and at rest (AES-256 or equivalent);
- Role-based access controls and the principle of least privilege;
- Regular security assessments, vulnerability scanning, and penetration testing;
- Staff confidentiality obligations and security awareness training;
- Incident detection, response, and breach notification procedures.

No system can be guaranteed completely secure. If we become aware of a personal data breach that is likely to result in a risk to your rights and freedoms, we will notify the relevant supervisory authority within 72 hours where required, and affected individuals where the risk is high, in accordance with GDPR Articles 33 and 34.

12. Your rights

Under GDPR and Norwegian data protection law, you have the following rights in respect of personal data we hold about you as Controller:

- **Right of access** — to obtain confirmation of whether we process your data and a copy of it;
- **Right of rectification** — to have inaccurate data corrected and incomplete data completed;
- **Right of erasure** ("right to be forgotten") — to have your data deleted in certain circumstances;
- **Right to restrict processing** — to limit how we use your data in certain circumstances;
- **Right to data portability** — to receive your data in a structured, commonly used, machine-readable format and to transmit it to another controller;
- **Right to object** — to processing based on legitimate interests, and at any time to processing for direct marketing purposes;
- **Right to withdraw consent** — where processing is based on consent;
- **Right not to be subject to automated decision-making** — see section 15.

To exercise any of these rights, please contact us using the details in section 17. We will respond within one month of receipt of your request. That period may be extended by up to two further months for complex requests, in which case we will tell you within the first month. We may need to verify your identity before responding.

Exercising your rights is free of charge, unless your request is manifestly unfounded or excessive, in which case we may charge a reasonable fee or decline to act on the request, as permitted by GDPR Article 12(5).

Inndeling 1.12 Complaints

If you are not satisfied with how we handle your personal data, you have the right to lodge a complaint with the Norwegian Data Protection Authority (Datatilsynet) at www.datatilsynet.no, or with the supervisory authority in the EEA Member State of your habitual residence, place of work, or place of the alleged infringement.

13. Cookies and similar technologies

We use cookies and similar technologies on the Platform and our website. These include:

- **Strictly necessary cookies** — required for the Platform to function (e.g. authentication, session management, security). These do not require consent;
- **Functional cookies** — used to remember your preferences and choices;
- **Analytics cookies** — used to understand how the Platform is used and to improve it (provided by Amplitude);
- **Marketing cookies** — used in limited circumstances and only with your consent.

Where required by section 2-7b of the Norwegian Electronic Communications Act and the EU ePrivacy Directive, we obtain your consent before placing non-essential cookies. You can manage your cookie preferences via the cookie banner displayed on first visit or by adjusting your browser settings.

A separate Cookie Policy with detailed information on each cookie used is available at [vidda.io/cookies] [link to be inserted].

14. Children

The Platform is not directed at children. We do not knowingly collect personal data from individuals under the age of 16 (or such higher age as is set by applicable national law). If you believe a child has provided us with personal data, please contact us using the details in section 17 and we will take steps to delete it.

15. Automated decision-making and profiling

We do not make decisions based solely on automated processing that produce legal effects concerning you or that similarly significantly affect you. We use limited profiling for analytics purposes (for example, understanding how Content is consumed across Buyer segments), but these activities do not produce such effects.

16. Changes to this Policy

We may update this Policy from time to time. Where the changes are material, we will notify you by email or by prominent notice on the Platform at least 30 days before the changes

take effect. The "Effective Date" at the top of this Policy indicates when it was last updated. We recommend that you review this Policy periodically.

17. How to contact us

For any questions, requests, or complaints about this Policy or our processing of your personal data, please contact us:

- **Email:** [privacy@vidda.io / support@vidda.io]
- Post: Vidda Solutions AS, Ostadalsveien 3 A, 0753 Oslo, Norway
- **Organisation number:** 834 081 652

You may also contact the Norwegian Data Protection Authority (Datatilsynet) at www.datatilsynet.no.