Dibbla as your platform partner

Dibbla AB, Stockholm, Sweden · Version 2026-09-22

What you can say about us

Page 1 may be sent to your own customers word for word. Page 2 is the detailed account, one point per commitment, and each point is published in full at dibbla.com/trust.

All data is stored in the EU

Compute, databases, object storage and backups run in Germany and Finland. No customer data leaves the EU/EEA, unless a transfer is covered by an adequacy decision or the EU Standard Contractual Clauses.

Dibbla is a Swedish company

Dibbla AB has its registered office in Stockholm and is subject to Swedish law, with the Swedish Authority for Privacy Protection (IMY) as supervisory authority. The servers are operated by Hetzner, a German company, in data centres in Germany and Finland.

GDPR is built in

Dibbla is the processor for the data in your application, under an Article 28 data processing agreement that is part of the Terms and in force the moment they are accepted. Your data is never used to train AI models and is not shared beyond the sub-processors the service needs, each published with its purpose, location and safeguard. AI features process nothing until you switch them on, and then only with the provider you chose.

Code is reviewed before it goes live

Every deployment requires a documented pre-deploy review against the OWASP Top 10, stored in your own repository, and every build is scanned for known vulnerabilities and leaked secrets. Your application is isolated from other customers', all traffic is encrypted, and secrets live outside the code and can never be read back out.

Your app is watched after it goes live

Scheduled checks run against your application as often as you choose, and an overnight agent reads its logs, source and check history and files a proposal with a diff when something needs fixing — both once you switch them on. It never deploys on its own: a second person approves or denies each proposal.

You own your data and your code

Source code, databases and files export in standard formats at any time, with one command and at no charge. There is no fee for switching provider or for leaving.

Text to use in an e-mail to your customers

Five sentences, nothing to fill in.

Our service is hosted on Dibbla, a Swedish platform with all data stored inside the EU (Hetzner, Germany and Finland). Dibbla AB is our data processor under a data processing agreement meeting Article 28 of the GDPR, Swedish law applies, and our data is never used to train AI models. Every deployment requires a documented security review before it goes live, and every build is scanned for known vulnerabilities. More information: dibbla.com/trust.

And the line for your privacy policy

The “where is the data processed” paragraph most privacy policies already have.

Our service is hosted by Dibbla AB, Stockholm, on servers within the EU. Dibbla acts as our data processor under a data processing agreement.

Dibbla as your platform partner

Dibbla AB, Stockholm, Sweden · Version 2026-09-22

Compliance in detail

Every point below is in production today and published in full at dibbla.com/trust, with the requirement it answers and the binding document that commits us.

GDPR

Regulation (EU) 2016/679

- You are the controller for your application's data; Dibbla is your processor, and never trains AI models on it.
- The Article 28 DPA is part of the Terms, in force on acceptance, with a Swedish version published alongside it.
- The public Sub-processor List is part of the DPA: tiers, an “applies when” column, 30 days' notice, a right to object.
- Compute, databases, storage and backups run on Hetzner in Nuremberg and Helsinki; nothing leaves the EU/EEA uncovered.
- Published retention: logs 180 days, AI prompts 30, a deleted row gone from every backup in 30, deletion confirmed on request.
- A breach affecting your data reaches you within 48 hours — inside the 72 hours you have as controller.
- Dibbla assists with rights requests; REVIEW.md records what personal data you hold, how one person is deleted and who receives it.

EU Data Act

Regulation (EU) 2023/2854, Chapter VI

- Notice at most two months, the switch completed within 30 days of it ending, export for at least 30 days after that.
- Source as git, databases as PostgreSQL dumps, buckets as files, configuration as dotenv — all from one dibbla export.
- No charge for terminating, switching, exporting or transferring data out, ahead of the date the regulation sets.
- Your own container from your own Dockerfile; every platform piece around it has a standard counterpart elsewhere.

Security

GDPR Art. 32 · ISO/IEC 27001:2022 Annex A

- Every organisation is isolated in data, network and secrets; authorisation is org-scoped and fails closed.
- TLS at the edge, in the cluster and on custom domains; secrets sit outside your code and are never readable back.
- Production access is least-privilege, reviewed and confidential; sign-in is federated, so no passwords are stored.
- Deployments and administrative actions are logged with the acting user for 180 days; an AI agent acts as the person behind it.
- Seven-day point-in-time recovery plus 30 nightly copies; backups are never edited, they age out.
- No deployment without a pre-deploy review report against the OWASP Top 10, kept as REVIEW.md in your repository.
- Every build is scanned in-cluster for known vulnerabilities and leaked secrets, the findings attached to the version.
- An incident process with classified response times; and, once you switch them on, scheduled checks and an overnight agent that files proposals a second person approves.

Two things Dibbla deliberately does not do

They belong to the application, not the platform, and guessing would break working applications. Dibbla's published checklist tells your coding agent how to take them.

- Filter your application's outbound network traffic. Restrict the URLs your own code fetches — point 8 of the checklist.
- Apply request-size or rate limits in front of your application. Rate-limit your own login, signup, reset and verification endpoints — point 6 of the checklist.

Standards, and the company behind the platform

ISO/IEC 27001:2022 Annex A

Controls aligned with ISO/IEC 27001:2022 Annex A. Dibbla AB is not certified.

“Aligned with” means each Annex A theme has a named owner, a written policy and a documented gap analysis, reviewed twice a year. No accredited certification body has audited anything: Hetzner's certified data centres certify the operator, not Dibbla.

Article 28(3)(h): Dibbla contributes to audits by you or an auditor you mandate, once per twelve months on 30 days' written notice, and sooner if a supervisory authority requires it.

Dibbla AB is a Swedish limited company registered in Stockholm; the infrastructure is operated by Hetzner Online GmbH in data centres in Germany and Finland.