← All resources

SECURITY & DEPLOYMENT · 10 MIN READ

Know where your data goes

ArkOffice architecture, security controls, model processing and deployment choices, for the people who review a system before trusting it.

ON THIS PAGE

- Scope & assurance
- Architecture & flows
- Deployment models
- Published controls
- Residency & AI models
- Data handling
- Governance
- Due diligence
- Questions & answers

EU-hosted core data
Published locations for ArkOffice account, content and file storage

Deployment choice
Managed EU cloud, customer cloud, on-premises and air-gapped

Configurable enterprise identity
SSO and role-based controls offered in enterprise deployments

Reviewable architecture
Sources, data flows and open verification questions identified

01 / SCOPE & ASSURANCE

Security starts with precision.

ArkOffice is one product family, but a standard hosted account and a custom enterprise installation do not necessarily share every integration, provider or control. The first security question is always: which deployment are we assessing?

Standard ArkOffice service

The publicly documented web service with named hosting, storage, model, safety-check and delivery providers. The self-serve privacy policy and processor register describe these data flows.

arkintel.com/processors

Enterprise deployment

Arkintel also offers managed European cloud, customer-controlled private cloud, local hardware and air-gapped deployments. Identity, enabled models, data paths, operations and assurance terms must be specified in the solution design.

arkintel.com/enterprise

Reading guide

"Published" means Arkintel describes a capability or control in its own materials. It does not mean an independent audit has verified that control. Enterprise features, operational guarantees and data paths depend on the contracted configuration.

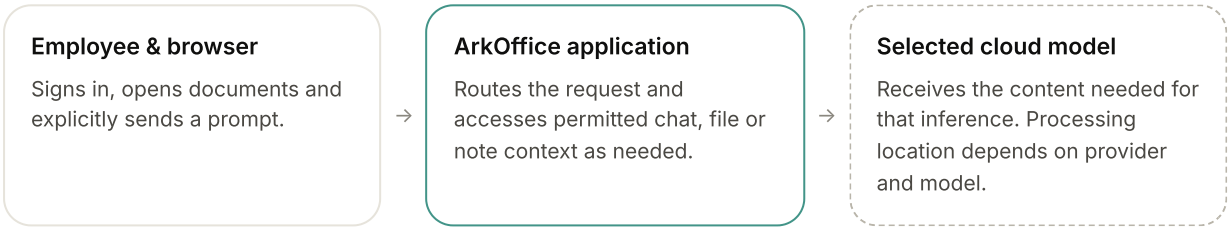
02 / ARCHITECTURE & FLOWS

Follow the request. Not just the server.

The central workspace, file storage and AI inference have different data paths. Understanding the boundaries is more useful than the blanket promise that everything happens in one location.

A cloud AI request, simplified.

ILLUSTRATIVE / SELF-SERVE FLOW



Solid teal: ArkOffice core · Dashed: external processing boundary. The safety-check host may also receive the scored prompt window before the selected model. An explanatory trust-boundary model, not a packet-level network diagram; exact routing and cross-border flows need a deployment-specific data-flow document.

Core & file storage

The privacy policy identifies Arkintel servers in Rotterdam for accounts, chats and notes. The register identifies IDrive e2 in Dublin for Drive file objects.

Delivery & identity

Global edge and frontend providers can handle connection metadata; chosen identity providers can handle authentication data. They are not the model host.

Inference & transcription

A submitted AI prompt is sent to the selected model host. The register separately documents safety scoring, speech-to-text and optional speaker separation.

Critical distinction

In the published standard-service documents, EU-only model selection does not by itself establish that every auxiliary service, metadata transfer and moderation flow remains exclusively in the EU. The Groq safety-check listing includes US and EEA processing. Confirm exact routing for any regulated or EU-only requirement.

03 / DEPLOYMENT MODELS

One suite. Different security perimeters.

Start with the level of control the organisation actually needs.

Managed EU cloud

Arkintel-operated infrastructure

Customer private cloud

Your cloud environment / VPC

On-premises

Hardware under your control

Air-gapped

Designed without internet paths

MANAGED / EU INFRASTRUCTURE

Speed without running the stack yourself.

Arkintel operates the suite on European infrastructure. A practical route for organisations evaluating everyday employee AI when their information policy permits the proposed managed-cloud data flows.

Infrastructure	Arkintel-operated European cloud
Model path	EU-hosted/open-weight options; other providers only as configured
Best evaluated for	Common office workflows and controlled trials, subject to classification
Verify before use	Tenancy, SSO, controls, subprocessors, retention, support and SLA

For private cloud, on-premises and air-gapped installations, the same questions are settled in the solution design. Not every architecture receives identical redundancy, backup, logging or operational responsibilities by default. A deployment design and agreed service schedule are required. Arkintel states that its managed cloud does not carry the additional certifications it requires for healthcare or privileged legal workloads.

04 / PUBLISHED CONTROLS

Controls you can actually discuss.

Arkintel publishes specific engineering and operational practices. These are useful inputs to a security review — but a published claim is not the same as a test report, certification or contractual commitment.

Encryption

HTTPS protects connections. The ArkOffice privacy policy describes server-side file-storage encryption and encryption at rest where compatible with the service. Processing may require content to be available in cleartext.

Published · Arkintel security + ArkOffice privacy

Identity & access

Arkintel offers enterprise SSO, OAuth2 and role-based access in scoped solutions; Keycloak is in its operated stack. Standard service sign-in and enterprise integrations are not the same contract or policy configuration.

Published / configurable · Enterprise & register

Edge protection

Arkintel describes a WAF, volumetric DDoS protection, attack detection and controlled production access. The self-serve privacy policy notes a WAF and denial-of-service controls as deployed.

Vendor-stated · Security & privacy

Resilience

The security site describes three active workload instances, failover, load balancing and two geographically distinct EU backup locations. Applicability and recovery targets need confirmation for each environment.

Vendor-stated architecture · Security page

Updates & isolation

Documented practices include isolated development, test and production environments, CI/CD with secret handling, health-checked rollout and traffic draining for new releases.

Vendor-stated operations · Security page

Monitoring & review

Arkintel describes monitoring, alerting, updates and security patching. Audit logs and tailored service levels are enterprise offerings; exact events, access, retention and reporting should be specified.

Published / enterprise-scoped · Arkintel

> **Security assurance is not a binary badge**
>
> Public materials do not establish an independently verified certification, penetration-test date, recovery-time objective, recovery-point objective or universal enterprise SLA. Ask for evidence and contractual schedules instead of treating these as proven.

05 / RESIDENCY & AI MODELS

European storage. Clear processing choices.

Data residency is a set of boundaries, not a switch. The location of stored files is distinct from the location of model inference, content-safety checks, identity systems and network metadata.

STORAGE LAYER

Where the standard service stores content.

The current ArkOffice privacy policy identifies Arkintel's own account, chat and note servers in Rotterdam, Netherlands. Its processor register lists IDrive e2 object storage for Drive files in Dublin, Ireland. EU storage locations are documented. Supplier domicile and metadata flows are separate matters.

INFERENCE LAYER

Where selected models process a prompt.

ArkOffice lists EU-region Mistral and Scaleway options alongside optional OpenAI, Anthropic and Google model hosts. Those hosts may process prompts outside the EEA depending on selection. No use of content for model-weight training is a stated contractual restriction, not a zero-retention guarantee.

> **EU-only mode: what must be verified**
>
> ArkOffice advertises EU-only model selection. Its disclosure also identifies Groq as a safety checker, and its register lists Groq processing in the US and EEA. Before claiming all processing is EU-contained, confirm whether the safety check is bypassed, replaced or region-locked in the intended configuration; likewise confirm edge, identity, transcription and telemetry flows. For a locally hosted or air-gapped installation, request a separate endpoint and network-boundary review.

06 / DATA HANDLING

Know what each promise does not mean.

The useful security conversation separates the protection that is stated from assumptions that would need a more detailed assessment. For the publicly documented standard service; enterprise terms and settings may differ.

Topic	What the documents support	What should not be inferred
Model training	Arkintel states it and its model hosts do not use submitted user content to train model weights, under supplier terms.	That every host immediately deletes prompts or keeps no abuse/safety logs.
EU storage	The standard service documents locate core account/chat data in Rotterdam and Drive files in Dublin.	That all ancillary metadata, inference and safety checks remain within the EU.
Encrypted content	HTTPS is used; storage encryption is described, with application-specific limitations.	That Arkintel cannot process readable content, or that customers always control encryption keys.
Deletion & retention	Account content is generally retained for the account's lifetime; post-contract export/deletion, backups, legal exceptions and flagged material have additional rules.	Instant deletion from every system or from third-party provider logs.
Human access	Production access is restricted to authorised staff. The policy describes authorised review of some flagged material.	That no operator or authorised reviewer can ever access customer content.
Compliance	Arkintel publicly describes GDPR-oriented design and security practices.	That a specific customer use case is automatically lawful, certified or regulator-approved.
Availability	Redundancy, backups and no-disruption deployment practices are described by Arkintel.	That a particular uptime percentage, RTO/RPO or restoration SLA is contractually guaranteed.

The ArkOffice Terms of Service state that self-serve backups are operational rather than a user backup service, and do not promise uninterrupted availability.

07 / GOVERNANCE

Infrastructure is only half the responsibility.

A credible enterprise setup pairs technical controls with policies, ownership and an operating model. This checklist describes what a customer and Arkintel should agree before sensitive use.

Useful AI. Accountable people.

Human verification remains essential for AI-assisted drafting, document interpretation, analysis and transcription. Approval rules, information classification and staff training are customer governance decisions — not things a model can safely supply on its own.

01

Information classification

Define what can enter the workspace, by data type, department, workflow and model. Do not assume that all material is approved simply because the server is in Europe.

02

Identity, roles & permissions

Agree who can log in, which identity provider is used, how groups and roles map to access, and how joiner/mover/leaver processes operate.

03

Processing & supplier review

Review the actual sub-processor list, international transfer tools, contract and DPA; scope approved models, transcription, safety checks and other supporting paths.

04

Logging, retention & response

Specify audit events, privileged access review, log retention, incident notification, content deletion and backup restore responsibilities in the agreed service terms.

05

Human approval & quality

Set source-checking and sign-off rules for factual outputs, finance, legal, policy, citizen-facing communication and meeting minutes. Test accuracy on real workflows.

06

Exit & continuity

Confirm export formats, migration assistance, retention after termination, business continuity, service ownership, recovery testing and contractual exit support.

08 / DUE DILIGENCE

Good questions make better deployments.

A short, concrete evidence request is more valuable than a generic security questionnaire. These are the items an ICT director, DPO or CISO should ask Arkintel to confirm for a proposed deployment.

#	Review checklist	What to confirm	✓
01	Deployment-specific architecture diagram	Hosts, networks, tenancy, gateways, model endpoints and all data transfers.	☐
02	Data residency & sub-processors	Exactly which data classes leave the selected region, including safety scoring and edge metadata.	☐
03	Information security assurance	Current certifications, audit reports, vulnerability and penetration-test summary, if available.	☐
04	Identity & authorisation	SSO, MFA, RBAC, provisioning, separation of duties and privileged operator access.	☐
05	Encryption & key ownership	TLS and at-rest methods, encryption key custody, rotation, secrets and access paths.	☐
06	Backup & recovery obligations	RPO, RTO, backup location, restore tests, business continuity and customer obligations.	☐
07	Logs & incident response	Audit event coverage, log retention, alerting, monitoring and breach-notification obligations.	☐
08	Retention, deletion & exit	Customer content, recordings, flagged prompts, support data, provider logs and export plan.	☐
09	Model & tool allowlist	Approved models, training exclusion, host retention, safety checks and tool/agent permissions.	☐
10	Contract & responsibilities	DPA, support and SLA, incident ownership, change notifications and security review cadence.	☐

Items above are verification requests, not claims that the relevant evidence is absent or that Arkintel cannot provide it. Publicly available information is not a substitute for a scoped technical review. For enterprise-specific answers or the full sub-processor picture, contact Arkintel's technical team. Security disclosures: security@arkintel.com

09 / QUESTIONS & ANSWERS

Six questions worth asking out loud.

Concise answers that preserve the distinction between what Arkintel publishes and what a customer needs to validate.

Does “EU-hosted” mean that no data ever reaches the US?

No. ArkOffice describes EU storage locations for its main application data and Drive objects. The published standard-service register separately names global network/identity services, optional non-EU model hosts and a safety-check provider operating in the US and EEA. Actual transfers must be reviewed against the proposed configuration.

Can we use confidential or personal information?

Only after classifying the information and evaluating the specific environment, contract, model hosts, data flows and permissions. Arkintel’s managed EU cloud may be suitable for some approved confidential workflows, but no general blanket guarantee is appropriate. Arkintel explicitly positions on-premises or air-gapped deployment for healthcare and privileged legal data and states its managed cloud lacks the extra certifications for those categories.

Does ArkOffice or a model provider train on our content?

Arkintel states that it does not train model weights on customer content and that its suppliers, under their terms as represented to Arkintel, do not use submitted prompts or files to train their weights. This does not mean that providers keep no inference logs or that flagged content is immediately deletable.

Does an air gap remove every security risk?

No. A properly designed air gap restricts network connectivity, but it does not automatically address compromised endpoints, software update media, administrator access, insider risk, backup handling or model errors. The boundaries and exceptions should be tested for the actual installation.

What certifications and guarantees can we cite?

Arkintel describes GDPR-oriented engineering and technical safeguards, but this document does not treat public website statements as an independent audit. Its self-serve terms explicitly do not promise uninterrupted service or a standard response time. Ask for any current certificates, relevant reports and a signed enterprise SLA before making contractual or regulatory claims.

Who operates and remains responsible for the system?

For an Arkintel-managed installation, Arkintel describes operating, monitoring and maintaining the platform. For customer private-cloud or on-premises environments, responsibilities around infrastructure, networks, backups, security, maintenance and incident handling must be allocated in the solution design and contract. The organisation remains responsible for its lawful use, information governance and human approval.

NEXT STEP

Questions after reading? Talk to the team.

We can walk through the details with your security, ICT or procurement colleagues and scope a setup around your information and users.

Start a conversation →

EMAIL
contact@arkintel.com

PHONE
+31 15 799 8447

OFFICE
Molengraaffsingel 12, Delft