

One Enterprise Workflow, Several Data Boundaries

Cloud and internal artificial intelligence choices for manufacturers operating across the European Union, United States and Greater China

Policy Brief | Research cutoff: 20 September 2026 (UTC+8)

Key Takeaways

1. Keep a common interface and approve data paths separately. Assess the data, purpose, recipient and access rights for each activity.
2. Govern internal AI by use case. Drafting and applicant screening require different checks; verify implementation dates by applicable category.
3. Check storage, inference and support separately. Verify the deployment configuration, contract and overseas access before procurement approval.

The decision behind a common platform

Consider a manufacturer sharing procedures, supplier records and employee documents across its operations. Management wants one internal assistant for knowledge retrieval and drafting. This is a deployment-design question with several legal layers. Pooling every record can create avoidable exposure; duplicating every application can raise operating costs. We assess three choices: what information can travel, what the assistant may do, and what the supplier actually provides. The central recommendation is a shared workflow with explicitly approved data paths, subject to business-specific validation.

1. Data permissions follow the transaction, beyond the server location

Under the General Data Protection Regulation (GDPR), lawful processing and a valid third-country transfer route are separate requirements. Appropriate contracts and safeguards must address the relevant recipients. A supplier's European region label is therefore only one input into approval.

Mainland China's 2024 cross-border rules exempt qualifying necessary human-resources transfers from three export mechanisms. They also provide exemptions for manufacturing data without personal information or important data. Other transfers require assessment against the applicable thresholds and exceptions; general protection duties remain. Reusing an employee archive for broad AI experimentation should undergo its own purpose and necessity review.

The United States adds a distinct national-security test. The Data Security Program covers specified transactions involving access to government-related or bulk sensitive personal data by countries of concern or covered persons. Some transactions are prohibited; others require security safeguards. Ordinary ancillary intra-group administration has a defined exemption, whose conditions need checking before restricting

routine payroll exchanges. California privacy obligations separately affect covered businesses and residents, illustrating why a federal-only map is incomplete.

Greater China is a business grouping. Hong Kong and Taiwan have their own data-protection regimes; mainland export thresholds should not be copied into their local compliance assessments.

Exhibit 1. The same platform requires separate activity-level decisions

Illustrative manufacturing workflow; selected rules at the research cutoff

Activity	Decision gate	Operational consequence
Share employee documents	Purpose, sensitive fields, exporter and recipient, transfer route	Limit accessible fields and document the approved route
Retrieve production knowledge	Personal/important data, confidentiality and recipient permissions	Create a reviewed knowledge collection
Rank job applicants	Intended use and applicable employment/AI requirements	Separate from the general drafting assistant
Enable overseas support	Who can access which records under which contract	Approve access explicitly and keep usable logs

Notes: Exemptions and sector rules can change the result. Source: Legal and regulatory sources listed below; Hale editorial synthesis.

2. A change in use can change the obligations

A manufacturer deploying a purchased assistant and a company providing a general-purpose model occupy different roles. European rules identify employment applications among potentially high-risk uses. Article 1(40)(b) of the 2026 amendment schedules Chapter III, Sections 1–3, except Article 6(5), from 2 December 2027 for high-risk systems under Article 6(2)/Annex III, and 2 August 2028 for Article 6(1)/Annex I systems. It also revises the AI-literacy obligation to require supporting measures, without guaranteeing an individual proficiency level. These are specific changes; they do not postpone every obligation.

In mainland China, the interim generative-AI measures exclude enterprise applications that do not provide services to the domestic public. Personal-information and other applicable duties still require separate assessment. Publishing an internal assistant to customers, or connecting it to personnel decisions, should therefore trigger a fresh review. The commercial benefit is a controlled expansion path: ordinary drafting can advance while consequential uses receive their own assessment and release conditions.

3. Buy an operating arrangement, then verify its boundaries

Microsoft's documentation distinguishes regional, Global and DataZone processing. A Global deployment may process prompts outside the storage geography; a European DataZone allows processing within the European Union. Stateful features can retain data separately from the model itself. These product

statements are useful procurement evidence, while the applicable contract and selected configuration determine the purchase.

Three deployment choices

Shared service with restricted inputs. Suitable when approved data can follow the proposed route. This simplifies administration while requiring a clear boundary on permitted inputs.

Regional knowledge stores and inference. Preserves a common interface with regional processing, at the cost of additional integration and testing.

Isolated deployment. May suit tightly constrained workloads. Allow for maintenance work and potentially reduced model choice.

Checks before approval. Record the required capability, permitted recipients, retention, incident response and exit route. Obtain the deployment geography, support-access matrix, subprocessors and retention/deletion terms, and test data export.

Exit costs. For covered services, Data Act switching charges, including switching-related data egress, end on 12 January 2027. Internal migration and application redesign still carry costs.

What to Watch

- Official European guidance implementing the amended high-risk timetable and classification rules.
- Mainland important-data notices and sector or free-trade-zone rules relevant to the actual factory and data.
- US Data Security Program designations, licences and clarification of relevant exemptions.
- Supplier changes to processing geography, subprocessors, retention and feature availability.
- Any expansion from document assistance into employment decisions or public-facing services.

Discuss cross-border deployment

Discuss how policy requirements affect an internal AI deployment with Hale. Defined use cases, jurisdictions and proposed data flows help identify questions for further legal and technical validation.

Sources

European Union. *General Data Protection Regulation, Regulation (EU) 2016/679*. 2016-04-27. Articles 5, 6, 28, 32, 44–49. [Source](#). Accessed 20 September 2026.

国家互联网信息办公室. *促进和规范数据跨境流动规定*. 2024-03-22. 第 3、5、7、8、10、13 条. [Source](#). Accessed 20 September 2026.

U.S. Department of Justice / eCFR. *28 CFR Part 202 — Data Security Program*. 2025-01-08. 202.205–210; 202.301; 202.401; 202.506; 202.601. [Source](#). Accessed 20 September 2026.

European Union. *AI Act, Regulation (EU) 2024/1689*. 2024-06-13. Articles 5, 6, 50; Annex III employment uses. [Source](#). Accessed 20 September 2026.

European Union. *Regulation (EU) 2026/1744 — Digital Omnibus on AI*. 2026-07-24 (公报). Article 1(5), 1(40)(b); Article 4. [Source](#). Accessed 20 September 2026.

Microsoft. *Data, privacy, and security for Foundry Models sold by Azure*. 动态产品文档；采集 2026-09-20. Global / DataZone processing; stored features; training use. [Source](#). Accessed 20 September 2026.

全国人大常委会／中国网信网转载. *中华人民共和国个人信息保护法*. 2021-08-20. 第 13、21、24、38-40、55 条及分页. [Source](#). Accessed 20 September 2026.

California Department of Justice. *California Consumer Privacy Act — public information*. 更新 2026-08-28. 消费者权利、适用企业、通知与服务商义务. [Source](#). Accessed 20 September 2026.

香港个人资料私隐专员公署. *Personal Data (Privacy) Ordinance overview*. 网页日期未注明. DPP2-4, 处理者保留、安全和用途. [Source](#). Accessed 20 September 2026.

台湾法务部全国法规资料库. *Personal Data Protection Act*. 以法条修订与施行栏为准. Article 21; 各条施行状态. [Source](#). Accessed 20 September 2026.

国家互联网信息办公室等七部门. *生成式人工智能服务管理暂行办法*. 2023-07-13. 第 2、22、24 条. [Source](#). Accessed 20 September 2026.

European Union. *Data Act, Regulation (EU) 2023/2854*. 2023-12-13. Chapter VI, Articles 23-31; Article 50. [Source](#). Accessed 20 September 2026.

European Commission, *Data Act explained*, Chapter VI, accessed 20 September 2026. [Source](#)