ChatGPT

Chính sách phân bổ đám mây (Cloud Placement Policy) cho Việt Nam

Tổng quan yêu cầu pháp lý hiện hành

Việc lưu trữ và xử lý dữ liệu trên hệ thống đám mây tại Việt Nam phải tuân thủ chặt chẽ các quy định pháp luật về an toàn thông tin, an ninh mạng và bảo vệ dữ liệu cá nhân. Các văn bản pháp luật chính bao gồm:

- **Luật An ninh mạng 2018** và **Nghị định 53/2022/NĐ-CP**: Yêu cầu doanh nghiệp cung cấp dịch vụ trên mạng viễn thông, Internet phải lưu trữ một số loại dữ liệu người dùng tại Việt Nam [1] [2]. Cụ thể, Nghị định 53 liệt kê **các loại dữ liệu bắt buộc lưu trữ trên lãnh thổ Việt Nam** bao gồm: *"Dữ liệu về thông tin cá nhân của người sử dụng dịch vụ tại Việt Nam; dữ liệu do người sử dụng dịch vụ tại Việt Nam tạo ra (vd: tên tài khoản, thời gian sử dụng, thông tin thẻ tín dụng, email, địa chỉ IP, số điện thoại...); và dữ liệu về mối quan hệ của người sử dụng dịch vụ tại Việt Nam"* [1]. Quy định này áp dụng cho các doanh nghiệp (kể cả nước ngoài) có thu thập, xử lý dữ liệu người dùng Việt Nam trên không gian mạng [2]. Như vậy, nếu tổ chức thuộc phạm vi điều chỉnh, **dữ liệu người dùng Việt Nam phải được lưu trữ onshore (trong nước)** theo yêu cầu của cơ quan chức năng.

- **Luật An toàn thông tin mạng 2015** và các văn bản hướng dẫn (Nghị định 85/2016/NĐ-CP, Thông tư 12/2022/TT-BTTTT,...): Thiết lập hệ thống phân loại mức độ an toàn cho hệ thống thông tin (5 cấp độ) và yêu cầu bảo vệ tương ứng. Hệ thống thông tin xử lý dữ liệu **càng quan trọng hoặc nhạy cảm** thì yêu cầu bảo mật càng cao, có thể bao gồm giới hạn về **địa điểm lưu trữ** (ví dụ: hệ thống cấp độ 4–5 chứa thông tin bí mật Nhà nước hoặc hạ tầng quốc gia **không được phép đặt trên môi trường cloud công cộng quốc tế** vì rủi ro an ninh).

- **Nghị định 13/2023/NĐ-CP về Bảo vệ Dữ liệu Cá nhân (PDPL)**: Quy định chi tiết về xử lý dữ liệu cá nhân và đặt ra yêu cầu nghiêm ngặt khi *chuyển dữ liệu cá nhân ra nước ngoài*. Điều 24 NĐ13 yêu cầu bên chuyển dữ liệu phải **đáp ứng các điều kiện nhất định và thông báo cho Bộ Công an** trước khi chuyển dữ liệu cá nhân của công dân Việt Nam ra nước ngoài [3]. Nói cách khác, **lưu trữ dữ liệu cá nhân trên máy chủ ở nước ngoài được coi là chuyển dữ liệu ra nước ngoài** và phải tuân thủ thủ tục pháp lý quy định [4]. Cụ thể, doanh nghiệp phải **lập hồ sơ Đánh giá tác động** (Data Protection Impact Assessment – DPIA) và gửi đến Cục An ninh mạng (A05, Bộ Công an) trong vòng 60 ngày kể từ khi bắt đầu chuyển dữ liệu [5], đồng thời **thông báo** cho Bộ Công an sau khi việc chuyển dữ liệu diễn ra [6]. Hồ sơ DPIA phải nêu rõ loại dữ liệu, mục đích chuyển, biện pháp bảo vệ, có **sự đồng ý của chủ thể dữ liệu** và có cam kết ràng buộc giữa bên chuyển và bên nhận dữ liệu [7] [8]. Nếu không tuân thủ, Bộ Công an có quyền yêu cầu ngừng chuyển dữ liệu ra nước ngoài [9].

- **Luật Dữ liệu 2024 (Data Act)** – có hiệu lực từ 1/7/2025: Đây là luật mới xác lập chủ quyền dữ liệu quốc gia. Luật quy định **"mọi dữ liệu phát sinh từ hoạt động của tổ chức, cá nhân Việt Nam được coi là tài nguyên thuộc chủ quyền Việt Nam và phải được lưu trữ, xử lý trong lãnh thổ Việt Nam, trừ trường hợp đặc biệt được cơ quan có thẩm quyền cho phép"** [10]. Như vậy, luật này thiết lập nguyên tắc chung là **ưu tiên lưu trữ dữ liệu onshore**, chỉ được đưa ra nước ngoài nếu

có sự chấp thuận đặc biệt. Luật Dữ liệu 2024 cũng yêu cầu việc chuyển dữ liệu ra nước ngoài phải **trải qua DPIA, đăng ký và được cơ quan quản lý phê duyệt** [11]. Quy định này nâng mức độ ràng buộc so với NĐ13/2023, thể hiện rõ xu hướng siết chặt việc bảo vệ dữ liệu và **bản địa hóa dữ liệu (data localization)** tại Việt Nam.

- **Luật/Các quy định khác**: Ngoài ra, cần kể đến **Luật Bí mật Nhà nước 2018** (cấm tiết lộ hoặc lưu trữ thông tin thuộc danh mục bí mật nhà nước trên hệ thống không được phép), các quy định chuyên ngành như của **Ngân hàng Nhà nước** (yêu cầu đánh giá rủi ro và xin chấp thuận khi sử dụng dịch vụ cloud cho ngân hàng theo Thông tư 09/2020/TT-NHNN), của **Bộ TT&TT** về an toàn hệ thống thông tin theo cấp độ, và các **hướng dẫn của Bộ Công an** về an ninh mạng cho dịch vụ đám mây phục vụ Chính phủ điện tử. Những văn bản này nhấn mạnh: hệ thống CNTT chứa dữ liệu nhạy cảm, quan trọng (ví dụ dữ liệu tài chính ngân hàng, y tế, giáo dục, dữ liệu quốc phòng...) cần được đặt tại các hạ tầng đáp ứng tiêu chuẩn an toàn cao, ưu tiên nhà cung cấp nội địa, và tuân thủ nguyên tắc chủ quyền dữ liệu [12].

Tóm lại, **các yêu cầu pháp lý chính** có thể khái quát thành: **(a)** Dữ liệu quan trọng của người Việt Nam phải lưu trữ tại Việt Nam, **(b)** Mọi hoạt động đưa dữ liệu ra khỏi biên giới phải qua thẩm định và được phép, **(c)** Hệ thống thông tin quan trọng phải đáp ứng tiêu chuẩn bảo mật tương ứng cấp độ, và **(d)** Tổ chức phải triển khai các biện pháp bảo vệ dữ liệu cá nhân, an ninh mạng theo quy định (quản lý truy cập, mã hóa, giám sát, lưu log, ứng phó sự cố, v.v.).

Quy tắc phân loại dữ liệu và lựa chọn môi trường lưu trữ (Rule-based)

Dựa trên các quy định pháp luật hiện hành, có thể thiết lập một bộ quy tắc "máy móc" để quyết định việc đặt dữ liệu/hệ thống trên môi trường nào (on-premises, cloud trong nước, cloud nước ngoài, hybrid). Dưới đây là tập các **rule** áp dụng:

1. **Dữ liệu cá nhân của công dân Việt Nam**: *Mặc định lưu trữ onshore*. Chỉ được lưu trữ trên hạ tầng nước ngoài (offshore cloud) nếu **đáp ứng đủ điều kiện của NĐ13/2023 và Luật Dữ liệu 2024** – bao gồm: có sự **đồng ý** của chủ thể dữ liệu, tiến hành **Đánh giá tác động** và gửi hồ sơ cho Bộ Công an, được phê duyệt hoặc không có yêu cầu chặn từ cơ quan quản lý [11] [13]. Nếu sử dụng dịch vụ đám mây nước ngoài (AWS, Google, Azure...) để lưu dữ liệu cá nhân người Việt, hành vi này **được xác định là chuyển dữ liệu xuyên biên giới** nên *phải thực hiện đúng thủ tục pháp lý*; nếu không sẽ vi phạm pháp luật về bảo vệ dữ liệu [4].

2. **Dữ liệu cá nhân nhạy cảm** (theo định nghĩa tại NĐ13/2023 – ví dụ: dữ liệu sức khỏe, sinh trắc học, thông tin tài chính, tôn giáo, vị trí...): *Phải được bảo vệ ở mức cao nhất*. **Ưu tiên lưu trữ on-prem hoặc cloud nội địa**. Nếu buộc phải lưu trên cloud nước ngoài, ngoài các điều kiện pháp lý như trên, cần **mã hóa mạnh** và triển khai các biện pháp kỹ thuật đặc biệt (xem Checklist ở dưới). Trong môi trường hybrid, dữ liệu cá nhân nhạy cảm nên được tách riêng và giữ tại hệ thống trong nước (ví dụ: mã hóa hoặc ẩn danh trước khi đưa lên cloud bên ngoài).

3. **Dữ liệu nội bộ không nhạy cảm** (không chứa thông tin cá nhân hay bí mật kinh doanh quan trọng, ví dụ: dữ liệu công khai, website, tài liệu thường): *Có thể linh hoạt lưu trữ on-prem, cloud nội địa hoặc cloud quốc tế*. Pháp luật không cấm lưu trữ loại dữ liệu này ở nước ngoài. Tuy nhiên, tổ chức vẫn nên

đánh giá rủi ro (về hiệu năng, chi phí, độ tin cậy) trước khi đưa dữ liệu ra nước ngoài. Dữ liệu công khai (public) có thể đặt trên cloud nước ngoài nếu chi phí và tiện ích tốt hơn.

4. **Thông tin/dữ liệu mật, quan trọng (ví dụ bí mật nhà nước, dữ liệu quan trọng của tổ chức)**: *Bắt buộc lưu trữ tại Việt Nam*. Các dữ liệu thuộc danh mục bí mật nhà nước hoặc dữ liệu trọng yếu cho an ninh quốc gia **không được phép lưu trên đám mây công cộng nước ngoài** vì rủi ro mất chủ quyền dữ liệu và truy cập trái phép bởi tổ chức nước ngoài. Những dữ liệu này chỉ nên nằm trên hạ tầng on-prem được bảo mật cao, hoặc trên **cloud do doanh nghiệp nội địa cung cấp** có chứng nhận phù hợp (ví dụ: cloud Chính phủ do Viettel, VNPT cung cấp). Đây là yêu cầu ngầm hiểu từ Luật An ninh mạng và luật Bí mật nhà nước.

5. **Dữ liệu ngành có quy định riêng**: Nếu tổ chức thuộc lĩnh vực có quy định chuyên ngành (ngân hàng, tài chính, y tế, viễn thông, giáo dục công lập…), phải tuân thủ thêm quy định của cơ quan quản lý ngành. Ví dụ: ngành ngân hàng yêu cầu **đánh giá rủi ro và xin phép** trước khi dùng dịch vụ cloud; ngành viễn thông yêu cầu nhà cung cấp cloud phải đăng ký dịch vụ theo Luật Viễn thông sửa đổi 2023, v.v. Chính sách phân bổ đám mây của tổ chức cần tham chiếu các văn bản này nếu áp dụng.

6. **Phân loại hệ thống theo mức độ quan trọng**: Trước khi quyết định đưa hệ thống ứng dụng lên cloud, cần xác định *mức độ ảnh hưởng khi hệ thống gián đoạn hoặc bị lộ dữ liệu*. Áp dụng nguyên tắc: hệ thống **càng quan trọng**, yêu cầu **càng thận trọng** khi chọn nền tảng cloud:

7. Hệ thống **Critical** (quan trọng cao): ưu tiên on-premises hoặc cloud nội địa; nếu dùng cloud public phải có phương án dự phòng (DR) trong nước và kiểm soát chặt chẽ.
8. Hệ thống **Moderate** (quan trọng vừa): có thể dùng mô hình hybrid hoặc cloud nội địa; cloud quốc tế chỉ dùng cho phần không chứa dữ liệu nhạy cảm và phải đảm bảo tuân thủ.
9. Hệ thống **Non-critical** (thấp): có thể triển khai trên cloud công cộng (kể cả offshore) để tối ưu chi phí, nhưng vẫn cần các biện pháp bảo mật cơ bản.

Các quy tắc trên cho phép hình thành ma trận quyết định cụ thể ở phần dưới. Lưu ý rằng **mọi ngoại lệ** (trường hợp muốn đưa dữ liệu bắt buộc onshore ra nước ngoài) phải được cấp có thẩm quyền duyệt bằng văn bản. Đồng thời, tổ chức cần lưu trữ bằng chứng tuân thủ (hồ sơ DPIA, văn bản chấp thuận, hợp đồng bảo mật với nhà cung cấp…) để sẵn sàng cung cấp khi kiểm tra.

Ma trận 1: Loại dữ liệu vs. Tùy chọn lưu trữ

Bảng sau phân loại các **nhóm dữ liệu** phổ biến và xác định liệu chúng được *phép lưu trữ* trên hạ tầng nào: **On-Premises (máy chủ nội bộ tại VN)**, **Public Cloud trong nước (Region tại VN của nhà cung cấp hoặc cloud do công ty nội địa)**, **Public Cloud ở nước ngoài**, và **Mô hình Hybrid** (kết hợp). Đồng thời liệt kê các *điều kiện/kiểm soát* nếu có.

Loại Dữ liệu	On-Prem (Nội bộ)	Public Cloud (VN)	Public Cloud (Nước ngoài)	Hybrid (Kết hợp)
Dữ liệu công khai (*Public, không nhạy cảm*)	✅ **Cho phép**. *(Ví dụ: thông tin trên website, tài liệu đã công bố.)* Không hạn chế.	✅ **Cho phép**. Không hạn chế.	✅ **Cho phép**. Không hạn chế pháp lý. Khuyến nghị đánh giá rủi ro (độ trễ, chi phí).	✅ **Cho phép**. Linh hoạt tùy nhu cầu hiệu năng, sao lưu.
Dữ liệu nội bộ nhạy cảm thấp (*Internal, không chứa PII hay bí mật*)	✅ **Cho phép**. Tuân thủ chính sách CNTT nội bộ.	✅ **Cho phép**. Nên chọn nhà cung cấp tuân thủ tiêu chuẩn bảo mật (ISO 27001…).	✅ **Cho phép**. **Điều kiện**: Đánh giá rủi ro bảo mật và pháp lý. Không có yêu cầu pháp lý đặc thù, nhưng nên mã hóa dữ liệu quan trọng.	✅ **Cho phép**. Cân nhắc lưu bản sao dữ liệu quan trọng on-prem để dự phòng.
Dữ liệu cá nhân (PII) – thường (*Thông tin cá nhân cơ bản của SV, phụ huynh, GV,…*)	✅ **Cho phép**. Phải áp dụng biện pháp bảo vệ dữ liệu cá nhân theo NĐ13 (quyền riêng tư, xóa dữ liệu khi có yêu cầu…).	✅ **Cho phép**. **Điều kiện**: Ký thỏa thuận xử lý dữ liệu (DPA) với nhà cung cấp cloud. Đảm bảo nhà cung cấp lưu trữ dữ liệu trên lãnh thổ VN.	⚠ **Có điều kiện**. *Không khuyến khích.* Chỉ được lưu nếu **đáp ứng NĐ13**: có **đồng ý** của người dữ liệu, lập **DPIA**, **thông báo Bộ CA** [13]. Cần **mã hóa** dữ liệu cá nhân trước khi lưu (đề phòng truy cập trái phép) và có biện pháp hạn chế truy cập từ nước ngoài.	⚠ **Có điều kiện**. Lựa chọn mô hình *hybrid*: giữ dữ liệu PII trong cơ sở dữ liệu trên máy chủ VN, chỉ đưa lên cloud các dữ liệu đã mã hóa/ẩn danh. Đảm bảo kênh truyền an toàn giữa on-prem và cloud.

Loại Dữ liệu	On-Prem (Nội bộ)	Public Cloud (VN)	Public Cloud (Nước ngoài)	Hybrid (Kết hợp)
Dữ liệu cá nhân nhạy cảm (*Sensitive PII: sức khỏe SV, thông tin tài chính, thông tin định danh quan trọng...*)	✅ **Cho phép**. Phải **mã hóa, hạn chế truy cập** nghiêm ngặt. Áp dụng đầy đủ biện pháp bảo vệ cho dữ liệu nhạy cảm (Điều 27, 28 NĐ13). Chỉ nhân sự được ủy quyền mới được truy cập.	✅ **Cho phép**. **Điều kiện**: Nên lưu trên **cloud nội địa** có chứng nhận an toàn. Ký DPA, đảm bảo nhà cung cấp không sao chép dữ liệu ra ngoài. Tiến hành **đánh giá bảo mật** định kỳ.	⚠ **Rất hạn chế**. *Tránh lưu trữ trên cloud nước ngoài trừ phi thật cần thiết.* Nếu buộc dùng, phải có **chấp thuận đặc biệt** (theo Luật Dữ liệu 2024) [10], làm DPIA và được phê duyệt. Bắt buộc **mã hóa mạnh** (ví dụ AES-256) và giữ khóa giải mã tại VN (Key Management nội bộ). Giám sát chặt chẽ truy cập.	⚠ **Có điều kiện**. Mô hình hybrid thường được khuyến nghị: dữ liệu nhạy cảm lưu on-prem hoặc cloud riêng tại VN; chỉ phân tích tổng hợp ẩn danh trên cloud công cộng. Nếu sử dụng hybrid, đảm bảo phần dữ liệu trên cloud đã được loại bỏ thông tin định danh cá nhân.
Dữ liệu mật, quan trọng cao (*Bí mật nhà nước, tài sản trí tuệ cốt lõi, dữ liệu tác nghiệp sống còn...*)	⛔ **Bắt buộc nội địa**. Chỉ lưu trữ trên hạ tầng on-prem có bảo mật cao hoặc mạng chính phủ. **Không đưa lên đám mây công cộng**. Tuân thủ Luật BMNN.	⚠ **Giới hạn**. Chỉ sử dụng nếu cloud đó thuộc mạng nội bộ Chính phủ hoặc nhà cung cấp được cấp phép đặc biệt. Yêu cầu ký kết thỏa thuận đảm bảo an ninh.	⛔ **Không cho phép**. Vi phạm nghiêm trọng nếu đưa loại dữ liệu này ra nước ngoài. Dữ liệu chiến lược quốc gia/nội bộ nằm ngoài kiểm soát pháp luật VN là không chấp nhận được [14] [15].	⚠ **Hybrid hạn chế**. Có thể dùng hybrid *đóng* (ví dụ: hạ tầng chính on-prem, cloud private nội địa làm DR). Tuyệt đối không đặt phần dữ liệu cốt lõi trên cloud công cộng nước ngoài.

Chú thích: ✅ = Được phép; ⚠ = Được phép với điều kiện/giới hạn; ⛔ = Không được phép (cấm theo chính sách). Điều kiện chi tiết về kiểm soát an ninh được liệt kê trong cột tương ứng hoặc trong Checklist ở cuối tài liệu.

Bảng trên cho thấy, **đối với dữ liệu cá nhân của sinh viên, phụ huynh, giáo viên trong lĩnh vực giáo dục** (PII) – nên ưu tiên lưu trữ tại hạ tầng nội địa (on-prem hoặc cloud Việt Nam). Nếu cần dùng dịch vụ đám mây toàn cầu (như Google Workspace, Microsoft 365 đặt máy chủ ở Singapore/EU/US), trường học **phải tuân thủ quy định chuyển dữ liệu cá nhân xuyên biên giới** nêu trên, nếu không sẽ có nguy cơ vi phạm

pháp luật Việt Nam [11] [12]. Thực tế, các chuyên gia cảnh báo doanh nghiệp Việt sử dụng SaaS quốc tế có thể vi phạm Luật An ninh mạng 2018 và NĐ 53/2022 do không đáp ứng yêu cầu lưu trữ dữ liệu tại VN [16]. Đặc biệt với **dữ liệu nhạy cảm trong giáo dục** (ví dụ: thông tin sức khỏe sinh viên, dữ liệu nghiên cứu quan trọng của trường), việc để trên cloud nước ngoài tiềm ẩn rủi ro bị truy cập bởi cơ quan nước ngoài (theo CLOUD Act của Mỹ) và nằm ngoài quyền tài phán Việt Nam [12]. Do vậy, **chính sách khuyến cáo mạnh mẽ**: dữ liệu cá nhân và dữ liệu nhạy cảm nên lưu trữ trong nước để đảm bảo tuân thủ và an ninh.

Ma trận 2: Mức độ quan trọng của hệ thống vs. Mô hình đám mây

Bên cạnh loại dữ liệu, **độ quan trọng của hệ thống** (system criticality) cũng quyết định lựa chọn kiến trúc đám mây. Ta phân hệ thống thành 3 cấp: **Cao (High)** – hệ thống trọng yếu, gián đoạn ảnh hưởng nghiêm trọng; **Trung bình (Moderate)** – hệ thống quan trọng vừa phải; **Thấp (Low)** – hệ thống không quan trọng.

Độ quan trọng của Hệ thống	On-Premises	Cloud nội địa	Cloud nước ngoài	Hybrid
Cao (Critical) *VD: Hệ thống quản lý sinh viên, tài chính kế toán cốt lõi; hệ thống thi cử quan trọng.*	**Ưu tiên**: Đặt on-prem hoặc trung tâm dữ liệu nội địa đáng tin cậy. Đảm bảo hệ thống đạt cấp độ 3-4 theo tiêu chí chính phủ (nếu là trường công) hoặc mức *High* theo NIST.	**Cho phép**: Nếu dùng cloud thương mại trong nước, phải đánh giá kỹ năng lực nhà cung cấp, đảm bảo SLA cao (99.9%), tuân thủ tiêu chuẩn ATTT và có hợp đồng đảm bảo an toàn.	**Hạn chế**: Không khuyến khích đặt hoàn toàn trên cloud nước ngoài do rủi ro gián đoạn đường truyền quốc tế và khó đảm bảo tuân thủ. Chỉ sử dụng nếu đã mã hóa toàn bộ dữ liệu và có phương án dự phòng on-prem.	**Khuyến nghị**: Mô hình hybrid là phù hợp – giữ phần core (CSDL, dịch vụ xác thực) on-prem, sử dụng cloud (có thể nước ngoài) cho thành phần ít nhạy cảm (ứng dụng front-end, CDN...). Đảm bảo có kế hoạch DR: sao lưu dữ liệu critical về on-prem thường xuyên.

Độ quan trọng của Hệ thống	On-Premises	Cloud nội địa	Cloud nước ngoài	Hybrid
Trung bình (Moderate) *VD: Hệ thống e-learning, website, ứng dụng quản trị có PII nhưng downtime ngắn chấp nhận được.*	**Có thể**: Triển khai on-prem nếu đã có sẵn hạ tầng, giúp kiểm soát dữ liệu. Tuy nhiên chi phí có thể cao, khó mở rộng.	**Tốt**: Cloud nội địa phù hợp để vừa tận dụng tài nguyên linh hoạt, vừa đáp ứng yêu cầu dữ liệu ở trong nước. Đảm bảo cấu hình HA (High Availability).	**Có thể**: Cho phép dùng cloud nước ngoài với **điều kiện** dữ liệu nhạy cảm (nếu có) được bảo vệ và tuân thủ PDPL. Nên chọn region gần Việt Nam để giảm độ trễ. Cần đánh giá rủi ro trường hợp cloud gián đoạn và chuẩn bị phương án thay thế.	**Phù hợp**: Mô hình hybrid linh hoạt – ví dụ, dữ liệu chính đặt trên cloud trong nước, còn server ứng dụng phụ trợ đặt trên cloud nước ngoài để tận dụng dịch vụ đặc thù. Đồng thời có kết nối an toàn giữa hai bên.
Thấp (Low) *VD: Hệ thống thử nghiệm, development, website công khai, dịch vụ không có dữ liệu nhạy cảm.*	**Tùy chọn**: On-prem nếu có sẵn máy chủ dư thừa; nếu không, có thể không cần đầu tư on-prem cho hệ thống phụ này.	**Tùy chọn**: Cloud nội địa vẫn tốt nếu chi phí cạnh tranh, hỗ trợ nhanh.	**Tốt**: Hoàn toàn có thể dùng cloud nước ngoài để tiết kiệm chi phí và tận dụng tính năng. Cần đảm bảo tuân thủ cơ bản (vd: không vô tình đưa dữ liệu cá nhân lên). Với hệ thống dev/test, cloud quốc tế linh hoạt rất hữu ích.	**Tùy chọn**: Hybrid ít được cần thiết cho hệ thống thấp, trừ khi muốn đồng bộ với môi trường production. Thông thường chọn một môi trường cloud phù hợp là đủ.

Giải thích: Hệ thống **Critical** yêu cầu độ tin cậy và bảo mật cao, do đó **ưu tiên triển khai tại hạ tầng mà tổ chức kiểm soát trực tiếp** (on-prem) hoặc cloud nội địa có cam kết chặt chẽ. Những hệ thống này thường *không chấp nhận rủi ro* từ việc phụ thuộc hoàn toàn vào hạ tầng nước ngoài (về pháp lý lẫn kỹ thuật). Hệ thống **Moderate** có thể cân bằng giữa on-prem và cloud, tùy mức độ dữ liệu nhạy cảm đi kèm. Hệ thống **Low criticality** thì **cloud-first** là xu hướng hợp lý để tối ưu chi phí và tài nguyên.

Ví dụ trong bối cảnh trường đại học: **Hệ thống quản lý sinh viên (có chứa nhiều dữ liệu cá nhân, điểm, tài chính)** được coi là *Critical* – nên đặt tại trung tâm dữ liệu của trường hoặc cloud trong nước đáng tin cậy, và sao lưu định kỳ. **Trang web công khai của trường** có thể coi là *Low* – có thể host trên cloud nước ngoài (CDN, hosting quốc tế) để tiết kiệm chi phí, miễn là nội dung không nhạy cảm. **Hệ thống e-learning** phục

vụ giảng dạy trực tuyến có thể là *Moderate* – có thể triển khai hybrid: dữ liệu học tập của sinh viên lưu ở DB trong nước, nhưng ứng dụng e-learning chạy trên cloud nước ngoài để tận dụng tính năng.

Cây quyết định (Decision Tree) cho việc đặt dữ liệu/hệ thống

Dựa trên hai ma trận trên, ta có thể diễn đạt logic lựa chọn môi trường **dưới dạng cây quyết định** như sau:

1. **Xác định loại dữ liệu mà hệ thống xử lý**: Nếu hệ thống chứa **dữ liệu bắt buộc nội địa** (theo luật) – ví dụ dữ liệu cá nhân người Việt, dữ liệu bí mật – **→ Chọn hạ tầng on-prem hoặc cloud trong nước.** *(Nhánh quyết định: "Dữ liệu thuộc loại hạn chế đưa ra nước ngoài?" – Nếu Có → Onshore)*. Ngược lại, nếu dữ liệu không bị hạn chế (public hoặc đã ẩn danh) – **→ Có thể cân nhắc cloud quốc tế**, chuyển sang bước 2.

2. **Dữ liệu cá nhân có nhạy cảm không?** Nếu **có dữ liệu cá nhân nhạy cảm** hoặc khối lượng lớn PII – **→ Ưu tiên on-prem hoặc cloud nội địa.** Chỉ chọn cloud nước ngoài nếu chấp nhận tuân thủ PDPL (DPIA, consent…) và triển khai các biện pháp mã hóa, kiểm soát nghiêm ngặt. *(Nhánh: "Chứa Personal Data của công dân VN?" – Nếu Có → Kiểm tra tiếp "Cloud nước ngoài có đáp ứng điều kiện PDPL không?" – Nếu Không → Không được phép offshore).* Nếu không có PII hoặc chỉ dữ liệu thông thường – → tự do hơn trong việc chọn môi trường.

3. **Xác định mức độ *critical* của hệ thống**: Nếu hệ thống thuộc hạng **Critical (quan trọng cao)** – **→ Chỉ triển khai trên hạ tầng tin cậy cao** (on-prem hoặc private/hybrid, *tránh thuần cloud công cộng quốc tế*). Nếu **Moderate** – → có thể chọn **hybrid hoặc cloud nội địa**, hoặc cloud quốc tế (với điều kiện bảo mật phù hợp). Nếu **Low** – → **Cloud-first** (kể cả quốc tế) là lựa chọn mặc định, miễn tuân thủ các yêu cầu tối thiểu.

4. **Đối chiếu lựa chọn qua ma trận**: Dựa trên kết quả từ bước 1–3, tham chiếu **Ma trận 1** (theo loại dữ liệu) và **Ma trận 2** (theo độ quan trọng) để xác định các tùy chọn cho phép. Nếu có hơn một tùy chọn (ví dụ: hệ thống moderate, dữ liệu không nhạy cảm có thể on-prem, cloud VN hoặc hybrid), hãy cân nhắc thêm về **mục tiêu kinh doanh và kỹ thuật**: yêu cầu hiệu năng, chi phí, khả năng mở rộng, năng lực quản trị hệ thống của tổ chức.

5. **Áp dụng điều kiện & biện pháp kiểm soát**: Với tùy chọn đã chọn, liệt kê các **điều kiện pháp lý cần tuân thủ** (ví dụ: cần thông báo Bộ CA khi dùng cloud ngoài; cần ký hợp đồng với nhà cung cấp dịch vụ….) và các **biện pháp kỹ thuật bắt buộc** (mã hóa, quản lý truy cập, lưu trữ log…). Các điều kiện/ biện pháp này được tổng hợp trong Checklist ở cuối tài liệu. Nếu tổ chức **không đáp ứng được các yêu cầu đi kèm** cho một tùy chọn nhất định, thì **phải chọn giải pháp khác an toàn hơn**. *(Ví dụ: nếu không thể đảm bảo mã hóa và xin phép khi đưa dữ liệu cá nhân ra nước ngoài, thì không được đặt dữ liệu đó trên cloud nước ngoài).*

6. **Phê duyệt và ghi nhận bằng chứng**: Mọi quyết định cần được phê duyệt bởi ban lãnh đạo hoặc bộ phận quản lý dữ liệu. Đồng thời, chuẩn bị các **tài liệu minh chứng**: Báo cáo phân loại dữ liệu/hệ thống, Biên bản phê duyệt lựa chọn cloud, Hồ sơ DPIA (nếu có), hợp đồng DPA với nhà cung cấp… Lưu trữ các tài liệu này để kiểm toán nội bộ hoặc thanh tra khi cần.

Quy trình trên có thể minh họa bằng lưu đồ dạng cây: bắt đầu từ câu hỏi "**Dữ liệu có thuộc loại phải lưu trữ tại VN không?**" → "**Hệ thống quan trọng mức nào?**" → "**Đáp ứng điều kiện bảo mật khi dùng cloud ngoài không?**"... cuối cùng đi đến **quyết định tối ưu** giữa: *On-prem, Cloud nội địa, Cloud nước ngoài hoặc Hybrid*. Mục tiêu là đảm bảo **tuân thủ luật pháp** trước tiên, sau đó tối ưu hóa lợi ích của điện toán đám mây.

Kiến trúc tham chiếu đề xuất

Dựa trên các lựa chọn về môi trường lưu trữ, dưới đây là **3 kiến trúc tham chiếu** từ bảo thủ đến cởi mở trong việc sử dụng đám mây, giúp tổ chức vừa **tuân thủ quy định** vừa đạt được hiệu quả vận hành:

1. Kiến trúc "Conservative" – ưu tiên nội địa và on-premises

Đây là cách tiếp cận thận trọng, phù hợp với tổ chức đặt yếu tố tuân thủ và bảo mật lên hàng đầu (ví dụ: trường đại học công lập, dữ liệu nhạy cảm cao). **Đặc điểm:**

- **Onshore-first:** Mọi dữ liệu quan trọng và hệ thống chính yếu đều được lưu trữ trên **máy chủ vật lý nội bộ** (on-premises) hoặc trên **dịch vụ cloud trong nước**. Ví dụ: Cơ sở dữ liệu sinh viên, hồ sơ nhân sự đặt tại data center của trường; nếu dùng cloud thì dùng của Viettel, VNPT, FPT đặt tại Việt Nam.
- **Hạn chế cloud quốc tế:** Hầu như *không sử dụng* cloud đặt ở nước ngoài cho dữ liệu hoặc hệ thống sản xuất. Cloud quốc tế (nếu có) chỉ dùng cho dịch vụ không chứa dữ liệu nhạy cảm, ví dụ: sử dụng CDN quốc tế cho website công khai, hoặc các công cụ học tập miễn phí, sau khi đã đánh giá không vi phạm quy định.
- **Kiểm soát chặt chẽ:** Mọi truy cập, truyền tải dữ liệu ra bên ngoài đều được kiểm duyệt. Hệ thống được cấu hình để **chặn** việc lưu dữ liệu vào các ứng dụng SaaS nước ngoài *nếu* chưa được phép. Ví dụ: chặn upload file chứa PII lên Google Drive cá nhân.
- **Ưu/nhược:** Kiến trúc này **đảm bảo tuân thủ tối đa** (khó vi phạm luật dữ liệu) và **tăng cường chủ quyền**. Tuy nhiên, nhược điểm là **chi phí đầu tư hạ tầng cao**, khó tận dụng hết tiện ích của đám mây (như mở rộng linh hoạt, dịch vụ AI, Big Data tiên tiến trên cloud quốc tế).

2. Kiến trúc "Balanced" – kết hợp linh hoạt (Hybrid Cloud)

Cách tiếp cận trung dung, cân bằng giữa tuân thủ và tận dụng lợi ích cloud. **Đặc điểm:**

- **Phân chia hệ thống theo dữ liệu:** Các thành phần/hệ thống được tách theo mức độ nhạy cảm. **Phần nhạy cảm lưu on-prem hoặc cloud VN**, phần ít nhạy cảm đưa lên public cloud. Ví dụ: Ứng dụng quản lý học tập: phần backend chứa DB sinh viên đặt tại server trường, còn phần ứng dụng web, nội dung e-learning chạy trên AWS/Singapore để tận dụng tính năng và băng thông.
- **Đồng bộ và bảo mật kết nối:** Kiến trúc hybrid đòi hỏi **kết nối an toàn** (VPN, kênh truyền riêng) giữa môi trường on-prem và cloud. Đảm bảo dữ liệu trao đổi được mã hóa. Có cơ chế **đồng bộ dữ liệu** cần thiết giữa hai bên gần thời gian thực.
- **Tuân thủ linh hoạt:** Nhờ giữ dữ liệu quan trọng trong nước, kiến trúc này **tuân thủ PDPL** (giảm phạm vi dữ liệu ra nước ngoài) nhưng vẫn cho phép sử dụng cloud quốc tế cho những phần được phép. Có thể đáp ứng yêu cầu Luật Dữ liệu 2024 bằng cách xin phép cho một phần nhỏ dữ liệu được chuyển (sau khi đã ẩn danh tối đa).
- **Ưu/nhược:** Kiến trúc hybrid **tối ưu hóa được chi phí và hiệu năng** – tận dụng cloud cho phần phù hợp, giảm tải đầu tư on-prem. Đồng thời **giảm thiểu rủi ro pháp lý** so với thuần cloud quốc tế.

Thách thức chính là **quản lý phức tạp hơn** (hai môi trường), cần kỹ năng tích hợp, và phải đảm bảo không có lỗ hổng ở giao diện giữa on-prem và cloud.

3. Kiến trúc "Cloud-first" – ưu tiên đám mây (nhưng vẫn tuân thủ)

Cách tiếp cận này hướng đến **tận dụng tối đa lợi ích của điện toán đám mây**, phù hợp cho tổ chức có nhu cầu đổi mới nhanh, chi phí hạ tầng thấp, nhưng phải **đi kèm biện pháp tuân thủ**. **Đặc điểm:**

- **Cloud tối đa, on-prem tối thiểu:** Phần lớn hệ thống, ứng dụng đều triển khai trên **dịch vụ cloud** (có thể bao gồm cả cloud quốc tế). Tổ chức chỉ duy trì on-prem cho những thứ bất khả kháng (ví dụ: hệ thống kế thừa cũ, hoặc một cụm máy chủ làm backup).
- **Multi-cloud, ưu tiên nội địa khi có thể:** Nếu dịch vụ cloud nội địa có sẵn tính năng, sẽ được ưu tiên. Chỉ dùng cloud nước ngoài cho những dịch vụ độc nhất hoặc có lợi thế vượt trội. Ví dụ: sử dụng Google Cloud BigQuery cho phân tích dữ liệu lớn, nhưng đặt máy ảo ứng dụng tại Viettel Cloud trong nước.
- **Tuân thủ bằng kỹ thuật và quy trình:** Để không vi phạm luật, kiến trúc cloud-first phải kết hợp **các biện pháp kỹ thuật** như: *mã hóa end-to-end* đối với dữ liệu lưu trên cloud nước ngoài (khóa do tổ chức giữ), *token hóa* dữ liệu cá nhân (chỉ lưu token trên cloud, dữ liệu gốc giữ tại một vault trong nước), **quản lý danh tính và quyền hạn chặt chẽ** trên môi trường cloud. Đồng thời phải thực hiện đầy đủ thủ tục pháp lý: thông báo, xin phép cơ quan chức năng về việc dùng cloud nước ngoài cho dữ liệu cá nhân (theo NĐ13/2023 và Luật Dữ liệu 2024).
- **Đảm bảo dự phòng:** Mặc dù cloud-first, tổ chức vẫn nên có **bản sao dự phòng** các dữ liệu quan trọng tại Việt Nam (on-prem nhỏ hoặc dịch vụ backup nội địa). Điều này để đề phòng tình huống xấu (nhà cung cấp cloud bị sự cố, hoặc có lệnh dừng chuyển dữ liệu từ Bộ Công an do vi phạm).
- **Ưu/nhược:** Kiến trúc cloud-first mang lại **sự linh hoạt, nhanh nhẹn** trong phát triển dịch vụ, **tiết kiệm chi phí đầu tư** ban đầu, dễ dàng áp dụng công nghệ mới. Nếu thực hiện tốt các biện pháp bảo mật, hệ thống vẫn an toàn và **tuân thủ ở mức chấp nhận được**. Tuy nhiên, rủi ro pháp lý có thể cao hơn hai kiến trúc trên – đòi hỏi tổ chức **kỷ luật** trong việc tuân thủ quy trình (đánh giá tác động, xin phép) và **giám sát liên tục** hoạt động của nhà cung cấp cloud (đảm bảo dữ liệu không bị lạm dụng). Kiến trúc này phù hợp nếu tổ chức có đội ngũ CNTT am hiểu về cloud và sẵn sàng chịu trách nhiệm quản lý bảo mật cloud.

Ba kiến trúc trên là các điểm mốc tham chiếu; trên thực tế tổ chức có thể tùy biến kết hợp các yếu tố để phù hợp nhu cầu. Điều quan trọng là **đảm bảo các nguyên tắc về dữ liệu nào được đặt ở đâu** đã nêu trong chính sách.

Mẫu chính sách Cloud Placement (trích 1-2 trang)

Dưới đây là **mẫu chính sách phân bổ dữ liệu/hệ thống lên đám mây** mà tổ chức (ví dụ một trường đại học) có thể ban hành, dựa trên phân tích ở trên:

Mục đích: Đảm bảo việc sử dụng dịch vụ điện toán đám mây tuân thủ pháp luật Việt Nam và bảo vệ an toàn cho dữ liệu của <Tên Tổ chức>, đặc biệt là dữ liệu cá nhân của sinh viên, giảng viên, cán bộ. Chính sách này đặt ra nguyên tắc để quyết định dữ liệu/hệ thống nào được phép đặt trên môi trường đám mây, ở địa điểm nào (trong hay ngoài nước).

Phạm vi áp dụng: Áp dụng cho toàn bộ dữ liệu, hệ thống thông tin của <Tổ chức>, bao gồm cả hệ thống do đối tác cung cấp dịch vụ cloud cho <Tổ chức>. Nhân sự và bên thứ ba tham gia xử lý dữ liệu của <Tổ chức> cũng phải tuân thủ chính sách này.

Định nghĩa chính: - *Dữ liệu cá nhân:* Thông tin về một cá nhân cụ thể (theo NĐ13/2023/NĐ-CP). Bao gồm dữ liệu cá nhân cơ bản và nhạy cảm (ví dụ: thông tin định danh, liên hệ, học tập của sinh viên; dữ liệu sức khỏe, tài chính nếu có). - *On-Premises:* Hệ thống máy chủ đặt tại cơ sở hạ tầng do <Tổ chức> quản lý trên lãnh thổ Việt Nam. - *Cloud nội địa:* Dịch vụ điện toán đám mây có trung tâm dữ liệu đặt tại Việt Nam, do đơn vị nội địa hoặc quốc tế cung cấp nhưng tuân thủ yêu cầu lưu trữ dữ liệu tại VN. - *Cloud nước ngoài:* Dịch vụ điện toán đám mây có trung tâm dữ liệu đặt ngoài lãnh thổ Việt Nam. - *Hệ thống Critical/Quan trọng:* Hệ thống thông tin mà khi gián đoạn hoặc lộ lọt dữ liệu sẽ ảnh hưởng nghiêm trọng đến hoạt động của <Tổ chức> hoặc quyền lợi của số đông cá nhân (tương đương mức độ 3-4-5 theo NĐ85/2016). - *Hybrid:* Mô hình kết hợp on-premises và cloud.

Chính sách chi tiết:

1. **Phân loại dữ liệu & hệ thống:** Tất cả dữ liệu phải được phân loại (công khai, nội bộ, cá nhân, nhạy cảm, mật) và hệ thống được xếp hạng mức độ quan trọng (Thấp/Trung bình/Cao) bởi Bộ phận Quản trị hệ thống & An toàn thông tin. Việc phân loại này phải được xem xét định kỳ hàng năm hoặc khi có hệ thống mới.

2. **Nguyên tắc đặt dữ liệu theo loại:**

3. **Dữ liệu bắt buộc lưu trữ trong nước:** Dữ liệu cá nhân của công dân VN, dữ liệu nhạy cảm, thông tin thuộc bí mật nhà nước **phải được lưu trên hạ tầng đặt tại Việt Nam** (on-prem hoặc cloud nội địa) [10]. **Không được** tự ý lưu những dữ liệu này trên dịch vụ cloud đặt ở nước ngoài (Google Drive, AWS, v.v.) nếu chưa đáp ứng các điều kiện luật định.
4. **Dữ liệu cá nhân thông thường:** Ưu tiên lưu trữ tại VN. Trường hợp cần xử lý trên cloud ngoài, **phải thực hiện quy trình phê duyệt** (xem Mục 3 dưới) trước khi chuyển. Đảm bảo tuân thủ Nghị định 13/2023 – bao gồm xin **sự đồng ý** của cá nhân liên quan và thực hiện **Đánh giá tác động**.
5. **Dữ liệu công khai hoặc không nhạy cảm:** Được phép lưu trữ trên cloud bất kỳ nếu đáp ứng yêu cầu an ninh kỹ thuật cơ bản. Tuy nhiên, <Tổ chức> khuyến khích sử dụng giải pháp nội địa (Make in Vietnam) khi có khả thi, phù hợp Nghị quyết 57/NQ-CP về ưu tiên nền tảng số Việt Nam [17].

6. **Dữ liệu nội bộ quan trọng:** (vd: tài liệu chiến lược, mã nguồn quan trọng) phải được bảo vệ và hạn chế truy cập. Nếu lưu trên cloud công cộng, phải mã hóa và kiểm soát quyền chặt chẽ, ưu tiên cloud nội địa.

7. **Quy trình phê duyệt sử dụng cloud nước ngoài cho dữ liệu nhạy cảm:** Trước khi lưu trữ **bất kỳ dữ liệu nào** thuộc loại hạn chế lên dịch vụ cloud nước ngoài, đơn vị đề xuất phải:

8. **Lập Hồ sơ Đánh giá Tác động Chuyển dữ liệu** (theo mẫu quy định của Bộ Công an) bao gồm phân tích loại dữ liệu, bên nhận, biện pháp bảo vệ, rủi ro và phương án giảm thiểu [18] [8].
9. **Trình hồ sơ cho Lãnh đạo <Tổ chức> và Bộ phận Pháp chế** xem xét. Nếu phê duyệt nội bộ, tiếp tục **gửi hồ sơ DPIA đến Cục A05 - Bộ Công an** trong vòng 60 ngày kể từ khi dự kiến chuyển dữ liệu [5].

10. Chỉ sau khi có **xác nhận chấp thuận hoặc không ý kiến phản đối** từ cơ quan quản lý, <Tổ chức> mới được tiến hành đưa dữ liệu lên môi trường cloud nước ngoài. Nếu nhận được yêu cầu ngừng từ cơ quan chức năng, phải dừng ngay việc chuyển và lưu trữ dữ liệu đó offshore [9].

11. Mọi hồ sơ, thông báo liên quan phải được lưu trữ làm bằng chứng tuân thủ.

12. **Lựa chọn môi trường theo cấp độ hệ thống:**

13. Hệ thống **Cấp độ Cao (Critical)**: Triển khai trên **máy chủ do <Tổ chức> quản lý hoặc cloud nội địa** có độ tin cậy cao. Không được phụ thuộc hoàn toàn vào cloud nước ngoài. Yêu cầu có phương án dự phòng trong nước.
14. Hệ thống **Cấp độ Thấp**: Được phép triển khai trên **cloud công cộng** (kể cả nước ngoài) sau khi đảm bảo không chứa dữ liệu thuộc loại hạn chế. Bộ phận An toàn thông tin cần cấu hình các biện pháp bảo mật phù hợp trên môi trường cloud (theo Checklist).
15. Hệ thống **Cấp độ Trung bình**: Xem xét theo từng trường hợp, có thể dùng mô hình **Hybrid** để cân bằng yêu cầu.

16. Trước khi triển khai hệ thống mới trên cloud, đội kiến trúc hạ tầng phải đối chiếu ma trận quyết định (Data x Cloud, Critical x Cloud) của <Tổ chức> và trình **Biên bản lựa chọn kiến trúc** cho Ban Công nghệ phê duyệt.

17. **Biện pháp bảo vệ và tuân thủ liên tục:**

18. Dữ liệu lưu trên bất kỳ môi trường nào cũng phải được **mã hóa phù hợp**, **sao lưu định kỳ**, và **giám sát truy cập**.
19. Bộ phận CNTT phải thiết lập cơ chế **theo dõi việc tuân thủ**: ví dụ, quét và phát hiện nếu có dữ liệu nhạy cảm bị đưa lên dịch vụ cloud không cho phép (Data Loss Prevention).

20. Định kỳ hàng năm, tiến hành **kiểm tra đánh giá** việc thực hiện chính sách: xem các hệ thống cloud đang dùng có vi phạm chính sách không, dữ liệu có đúng nơi quy định không. Kết quả báo cáo cho Ban Giám đốc.

21. **Trách nhiệm:** Mọi nhân sự của <Tổ chức> khi sử dụng dịch vụ điện toán đám mây phải tuân thủ chính sách này. Bộ phận Quản lý Dữ liệu cùng Phòng CNTT chịu trách nhiệm hướng dẫn và kiểm tra. Vi phạm chính sách (đưa dữ liệu trái phép lên cloud nước ngoài, v.v.) sẽ bị xử lý kỷ luật và phải khắc phục ngay.

22. **Hiệu lực:** Chính sách có hiệu lực từ <ngày ban hành> và được cập nhật khi pháp luật hoặc môi trường công nghệ thay đổi (ví dụ: khi Luật Bảo vệ Dữ liệu cá nhân mới có hiệu lực, chính sách sẽ được rà soát bổ sung).

(Chính sách dài ~2 trang, có thể rút gọn hoặc chi tiết thêm tùy thuộc tình hình cụ thể của tổ chức. Phần phụ lục có thể bao gồm bảng phân loại dữ liệu và quy trình xin phép).

Checklist biện pháp kỹ thuật & kiểm soát yêu cầu

Cuối cùng, để đảm bảo việc triển khai theo chính sách được an toàn, dưới đây là **checklist các kiểm soát kỹ thuật** mà tổ chức cần áp dụng khi sử dụng cloud:

- **Quản lý định danh & quyền truy cập (IAM):** Thực hiện nguyên tắc *least privilege* trên môi trường cloud. Tích hợp xác thực tập trung (SSO) nếu khả thi. Bật xác thực đa yếu tố (MFA) cho tài khoản quản trị. Định kỳ soát lại quyền và khóa các tài khoản không dùng. Đối với cloud nước ngoài, cần cơ chế kiểm soát để đảm bảo chỉ nhân sự được ủy quyền ở VN mới truy cập dữ liệu nhạy cảm.

- **Mã hóa dữ liệu:** Mã hóa dữ liệu **at-rest** trên cloud (sử dụng các công cụ mã hóa đĩa, database encryption do nhà cung cấp cung cấp hoặc tự mã hóa trước khi upload). Đối với dữ liệu nhạy cảm, sử dụng mã hóa end-to-end; xem xét giải pháp *Bring Your Own Key* (BYOK) hoặc *Hold Your Own Key* – tự quản lý khóa mã hóa để nhà cung cấp cloud không tự ý giải mã được [12]. Mã hóa mạnh khi truyền (HTTPS/TLS) giữa on-prem và cloud.

- **Quản lý khóa (Key Management):** Lưu trữ khóa mã hóa trong **KMS nội bộ hoặc HSM** đặt tại VN. Hạn chế lưu khóa giải mã trên hạ tầng cloud nước ngoài. Thiết lập quy trình quản lý vòng đời khóa (tạo, phân quyền sử dụng, xoá khóa khi không dùng). Kiểm soát chặt việc truy cập tới hệ thống quản lý khóa.

- **Ghi log và giám sát:** Kích hoạt **logging** đầy đủ trên các dịch vụ cloud (nhật ký truy cập, cấu hình, hoạt động người dùng). Thiết lập chuyển log về hệ thống tập trung của <Tổ chức> (SIEM) để giám sát. Lưu trữ log tối thiểu 12 tháng (hoặc theo quy định) để phục vụ điều tra sự cố và kiểm toán. Đảm bảo log cloud của hệ thống quan trọng không được lưu duy nhất ở nước ngoài – nên có bản sao tại VN.

- **Giám sát an toàn & Phát hiện xâm nhập:** Triển khai các công cụ **giám sát bảo mật trên cloud** (Cloud Security Posture Management – CSPM, Cloud Trail/Monitor) để phát hiện cấu hình rủi ro. Sử dụng IDS/IPS hoặc dịch vụ phát hiện xâm nhập có sẵn để cảnh báo hoạt động bất thường. Đối với hybrid, cần giám sát cả đường truyền kết nối.

- **Data Loss Prevention (DLP):** Áp dụng giải pháp DLP để ngăn chặn việc **rò rỉ dữ liệu**. Cấu hình các chính sách DLP: ngăn upload thông tin cá nhân nhạy cảm lên dịch vụ cloud không được phép (dựa trên nhận diện mẫu số CMND/CCCD, email sinh viên, v.v.), chặn gửi email ra bên ngoài có chứa dữ liệu nhạy cảm trừ khi được mã hóa. DLP cũng giúp phát hiện sớm vi phạm chính sách cloud placement (ví dụ: người dùng cài ứng dụng đồng bộ dữ liệu nội bộ lên cloud cá nhân).

- **Sao lưu (Backup) & Phục hồi:** Thiết lập cơ chế backup định kỳ các dữ liệu/ứng dụng trên cloud về một **điểm lưu trữ tại Việt Nam** (on-prem hoặc cloud nội địa khác). Đối với hệ thống critical, giữ ít nhất 1 bản backup offline. Kiểm thử kế hoạch khôi phục thảm họa (DR) định kỳ để đảm bảo có thể chuyển hệ thống về on-prem hoặc cloud dự phòng khi cần (đặc biệt quan trọng nếu dùng cloud nước ngoài, phòng trường hợp bị yêu cầu ngừng chuyển dữ liệu hoặc gặp sự cố nhà cung cấp).

- **Ứng phó sự cố (IR):** Xây dựng **kịch bản ứng phó sự cố an ninh mạng trên môi trường cloud**: ví dụ, lộ dữ liệu từ bucket S3, tài khoản cloud bị xâm nhập, v.v. Quy định rõ ai liên hệ (bao gồm cả liên

hệ nhà cung cấp cloud), các bước cô lập, thu thập bằng chứng log. Trong quá trình xử lý sự cố, tuân thủ nghĩa vụ báo cáo cơ quan chức năng (theo Luật An ninh mạng, phải thông báo cơ quan quản lý trong 24h nếu sự cố nghiêm trọng). Đối với dữ liệu cá nhân, thông báo các cá nhân bị ảnh hưởng theo yêu cầu của luật.

- **Thỏa thuận pháp lý với nhà cung cấp:** Đảm bảo đã ký **Hợp đồng dịch vụ & Phụ lục xử lý dữ liệu (DPA)** với nhà cung cấp cloud, trong đó ràng buộc: nhà cung cấp phải tuân thủ Luật Việt Nam về bảo vệ dữ liệu cá nhân, không chuyển dữ liệu của <Tổ chức> cho bên thứ ba nếu không được phép, hợp tác khi có yêu cầu kiểm tra. Điều khoản về vị trí lưu trữ: xác định rõ dữ liệu được lưu tại vùng nào. Đây là cơ sở pháp lý quan trọng bảo vệ <Tổ chức> [19].

- **Kiểm tra tuân thủ định kỳ:** Tổ chức thực hiện **audit nội bộ** hoặc thuê đánh giá độc lập định kỳ (ví dụ hàng năm) đối với hạ tầng cloud: kiểm tra cấu hình theo tiêu chuẩn (CIS Benchmark for Cloud), kiểm thử thâm nhập (pentest) với các ứng dụng trên cloud, rà soát việc phân loại dữ liệu có đúng nơi. Báo cáo audit phải nêu rõ điểm chưa phù hợp để khắc phục. Đặc biệt, kiểm tra xem dịch vụ cloud nước ngoài có còn đáp ứng điều kiện pháp luật mới ban hành hay không (ví dụ Luật Bảo vệ DL cá nhân 2025...).

Những biện pháp trên giúp tạo lớp phòng thủ vững chắc cho dữ liệu khi **"lên mây"**. Việc tuân thủ chính sách và thực hiện đầy đủ các kiểm soát sẽ không chỉ giúp tổ chức **tránh vi phạm pháp luật** (tránh nguy cơ bị phạt, bị yêu cầu ngừng dịch vụ) [11] [20], mà còn **nâng cao uy tín** về bảo mật, bảo vệ quyền riêng tư của người dùng. Trong bối cảnh chủ quyền số ngày càng được coi trọng, <Tổ chức> cần coi việc **làm chủ dữ liệu** là ưu tiên chiến lược – bảo đảm dữ liệu của mình luôn trong tầm kiểm soát và tuân thủ luật pháp Việt Nam [14] [15].

Nguồn tham khảo: Luật An ninh mạng 2018; NĐ 53/2022/NĐ-CP; NĐ 13/2023/NĐ-CP; Luật Dữ liệu 2024; Tạp chí An toàn thông tin [1] [13]; Hướng dẫn của Hilo Group về chủ quyền dữ liệu [10] [12]; Chuyên gia DPO.vn về chuyển dữ liệu lên cloud [4]; cùng các văn bản chuyên ngành liên quan.

---

[1] [2] [3] [13] Một số quy định pháp lý hiện hành tại Việt Nam liên quan đến bản địa hóa dữ liệu | An toàn thông tin
https://antoanthongtin.vn/tin/mot-so-quy-dinh-phap-ly-hien-hanh-tai-viet-nam-lien-quan-den-ban-dia-hoa-du-lieu

[4] Lưu Trữ Đám Mây Nước Ngoài Có Phải Là Chuyển Dữ Liệu Cá Nhân Xuyên Biên Giới?
https://dpo.vn/luu-tru-dam-may-nuoc-ngoai-co-phai-la-chuyen-du-lieu-ca-nhan-xuyen-bien-gioi/

[5] [6] [7] [8] [9] [18] Nghị định 13/2023/NĐ-CP bảo vệ dữ liệu cá nhân mới nhất
https://thuvienphapluat.vn/van-ban/Cong-nghe-thong-tin/Nghi-dinh-13-2023-ND-CP-bao-ve-du-lieu-ca-nhan-465185.aspx

[10] [11] [12] [14] [15] [16] [17] [19] [20] Nguy cơ vi phạm pháp luật khi doanh nghiệp sử dụng dịch vụ nước ngoài – Công ty Cổ Phần Dịch Vụ T-VAN HILO
https://hilo.com.vn/blogs/news/nguy-co-vi-pham-phap-luat-khi-doanh-nghiep-su-dung-dich-vu-nuoc-ngoai