ChatGPT

Hướng dẫn tuân thủ Public Cloud tại Việt Nam

A) Bản đồ pháp lý liên quan đến Public Cloud tại Việt Nam

Trước tiên, doanh nghiệp cần nhận diện đầy đủ các văn bản pháp luật ảnh hưởng trực tiếp hoặc gián tiếp đến việc sử dụng dịch vụ **điện toán đám mây công cộng (Public Cloud)**. Bảng dưới đây tổng hợp các nguồn luật chính, phạm vi áp dụng, các quy định cụ thể về dữ liệu/cloud, nghĩa vụ chính và tác động đối với việc dùng cloud của nhà cung cấp nước ngoài và trong nước:

Bảng: "Bản đồ pháp lý" cho Public Cloud tại Việt Nam

Luật An ninh mạng 2018 (số 24/2018/QH14, hiệu lực 01/01/2019)	Quốc hội	Tất cả cơ quan, tổ chức, cá nhân; đặc biệt DN cung cấp dịch vụ trên mạng viễn thông, Internet tại VN (kể cả nước ngoài)	Điều 26 yêu cầu **doanh nghiệp cung cấp dịch vụ trên mạng** phải **xác thực thông tin người dùng, bảo vệ tài khoản; gỡ bỏ thông tin vi phạm; lưu trữ log;** và đặc biệt khoản 3 quy định *DN thu thập, xử lý dữ liệu về thông tin cá nhân, quan hệ người dùng, dữ liệu người dùng tạo ra tại VN* **phải lưu trữ những dữ liệu này tại Việt Nam**, đồng thời **DN nước ngoài thuộc diện này phải đặt chi nhánh hoặc VPĐD tại VN** [1].	**– Xác thực, bảo mật thông tin tài khoản người dùng**; **cung cấp thông tin người dùng cho cơ quan an ninh mạng khi có yêu cầu bằng văn bản** [2] [3]. – **Ngăn chặn, xóa nội dung vi phạm** trong 24h theo yêu cầu; **lưu nhật ký hệ thống** phục vụ điều tra theo thời gian Chính phủ quy định [3]. – **Không cung cấp dịch vụ cho tổ chức, cá nhân** đăng tải thông tin vi phạm khi có yêu cầu từ Bộ CA hoặc Bộ TT&TT [4]. – **Lưu trữ dữ liệu người dùng VN trên lãnh thổ VN** (dữ liệu cá nhân, dữ liệu về mối quan hệ người dùng, dữ liệu do người dùng tạo ra) trong thời gian nhất định (theo hướng dẫn của CP) [1].	**Cloud của CSP nước ngoài:** Nếu CSP cung cấp dịch vụ **thu thập, xử lý dữ liệu người dùng VN** (ví dụ mạng XH, dịch vụ lưu trữ/sharing dữ liệu trực tuyến…) thì có thể thuộc diện phải **lưu dữ liệu tại VN và đặt hiện diện thương mại** theo yêu cầu của Bộ CA [1]. **Sau khi có yêu cầu chính thức**, CSP nước ngoài phải tuân thủ trong 12 tháng (có thể gia hạn 30 ngày do sự kiện bất khả kháng) và lưu dữ liệu tối thiểu 24 tháng [6] [7]. Danh mục **dữ liệu phải lưu** gồm: thông tin cá nhân người dùng; dữ liệu do người dùng tạo (tên TK,	Luật ANM 2018, Điều 26 [1] [3]; Nghị định 53/2022/NĐ-CP (Hướng dẫn Luật ANM) [10] [9].

			thời gian sử dụng, thẻ tín dụng, email, địa chỉ IP đăng nhập, số ĐT đăng ký…); dữ liệu về mối quan hệ của người dùng (bạn bè, nhóm) [8]. Danh mục **dịch vụ thuộc diện điều chỉnh** gồm 10 loại: viễn thông, **lưu trữ và chia sẻ dữ liệu trên mạng (cloud storage)**, cung cấp tên miền, TMĐT, thanh toán trực tuyến, trung gian thanh toán, dịch vụ vận tải kết nối qua mạng, mạng XH/ truyền thông, trò chơi online, dịch vụ email/chat/ voice/video online [9]. **Cloud nội địa:** CSP trong nước cung cấp dịch vụ tại VN cũng phải **lưu trữ**
		 – **DN nước ngoài thuộc diện phải lưu trữ dữ liệu** theo trên thì **phải đặt chi nhánh hoặc VPĐD tại Việt Nam** [5].	

Văn bản	Cơ quan ban hành	Phạm vi áp dụng	Quy định liên quan đến cloud/ data	Nghĩa vụ chính	Ảnh hưởng đối với cloud nước ngoài vs. nội địa	Nguồn
					các dữ liệu người dùng VN như trên (tại VN) nếu thuộc loại hình dịch vụ bị điều chỉnh; đồng thời tuân thủ các nghĩa vụ về an ninh mạng (xác thực, gỡ nội dung vi phạm, cung cấp thông tin người dùng khi được yêu cầu...) tương tự DN nước ngoài [2] [3].	

Nghị định 53/2022/ NĐ-CP (15/08/2022, hiệu lực 01/10/2022) – Hướng dẫn Luật An ninh mạng	Chính phủ	Áp dụng cho doanh nghiệp **trong và ngoài nước cung cấp dịch vụ trên mạng** tại VN; quy định chi tiết về **loại dữ liệu phải lưu trữ, dịch vụ thuộc phạm vi, thời gian lưu trữ và thủ tục yêu cầu** theo Luật ANM.	– Xác định **danh mục dữ liệu buộc lưu trữ tại VN** (như trên: dữ liệu cá nhân, dữ liệu do người dùng tạo, dữ liệu về mối quan hệ người dùng) [8] và **danh sách dịch vụ** phải lưu trữ dữ liệu (10 loại dịch vụ trực tuyến phổ biến) [9] . – Quy định **điều kiện kích hoạt yêu cầu lưu trữ**: Bộ CA có thể yêu cầu DN nước ngoài lưu trữ dữ liệu + đặt chi nhánh/VPĐD tại VN nếu *dịch vụ của họ bị sử dụng để vi phạm ANM Việt Nam* **và** *DN không hợp tác, không xử lý đầy đủ vi phạm khi được cơ quan A05 (Bộ CA) yêu cầu* [11] . – Thời	**– Lưu trữ nội địa:** CSP nước ngoài nằm trong danh mục dịch vụ nêu trên cần chuẩn bị phương án lưu trữ dữ liệu tại VN (VD: thuê trung tâm dữ liệu VN, hợp tác với CSP trong nước) để sẵn sàng tuân thủ nếu có yêu cầu chính thức. Nếu không tuân thủ, có rủi ro bị **đình chỉ cung cấp dịch vụ tại VN** theo Luật ANM. – **Hiện diện thương mại:** CSP nước ngoài phải cân nhắc việc **thành lập VPĐD/chi nhánh** khi kinh doanh lâu dài tại VN, vừa đáp ứng NĐ 53, vừa thuận tiện cho việc quản lý khách hàng và tuân thủ các luật khác (thuế, viễn thông...). – **Cloud nội địa:** Các CSP Việt Nam đương nhiên đã đặt hạ tầng	NĐ 53/2022/ NĐ-CP, Điều 1-5 [11] [6] ; Luật ANM 2018, Điều 26.3 [1] .

Văn bản	Cơ quan ban hành	Phạm vi áp dụng	Quy định liên quan đến cloud/ data	Nghĩa vụ chính	Ảnh hưởng đối với cloud nước ngoài vs. nội địa	Nguồn
			hạn tuân thủ: DN phải **hoàn thành lưu trữ dữ liệu tại VN và thiết lập hiện diện trong 12 tháng** từ khi có yêu cầu; dữ liệu phải được lưu tối thiểu **24 tháng** [6]. – Quy trình: Bộ CA (Bộ trưởng) ban hành quyết định yêu cầu; DN có thể được gia hạn 30 ngày nếu có sự kiện bất khả kháng [6].	tại VN nên đáp ứng yêu cầu lưu trữ dữ liệu nội địa dễ dàng; tuy nhiên vẫn cần **cơ chế lưu trữ và bảo vệ dữ liệu người dùng trong tối thiểu 24 tháng** (có thể cần tăng cường năng lực lưu trữ log, CSDL người dùng). – NĐ 53 cũng làm rõ **thẩm quyền của Bộ CA** trong thanh tra, kiểm tra việc tuân thủ ANM; do đó CSP trong nước và các khách hàng dùng cloud phải sẵn sàng hợp tác cung cấp thông tin khi được yêu cầu [2].		

Nghị định 13/2023/NĐ-CP về Bảo vệ Dữ liệu Cá nhân (ban hành 17/4/2023, hiệu lực 01/7/2023)	Chính phủ	Áp dụng rộng, bao gồm: – **Cơ quan, tổ chức, cá nhân Việt Nam**; – **Tổ chức, cá nhân nước ngoài** tại VN; – **Tổ chức, cá nhân VN hoạt động ở nước ngoài**; – **Tổ chức, cá nhân nước ngoài** trực tiếp tham gia hoặc có liên quan đến **xử lý dữ liệu cá nhân tại VN** [12] . *Nghĩa là mọi hoạt động xử lý dữ liệu cá nhân (DLCN) công dân VN, bất kể chủ thể ở đâu, đều thuộc phạm vi.*	– **Định nghĩa DLCN:** Thông tin gắn với một cá nhân cụ thể hoặc giúp định danh cá nhân đó; bao gồm **DLCN cơ bản** (ví dụ: họ tên, ngày sinh, giới tính, địa chỉ, số ĐT, ảnh, số định danh/CCCD, tình trạng hôn nhân, thông tin tài khoản số, lịch sử hoạt động mạng…) và **DLCN nhạy cảm** (ví dụ: quan điểm chính trị/tôn giáo, tình trạng sức khỏe đời tư, thông tin về nguồn gốc chủng tộc, dữ liệu di truyền, đặc điểm sinh học riêng, đời sống tình dục, thông tin về tội phạm, dữ liệu khách hàng tài chính, thông	– **Phân loại vai trò:** NĐ 13 xác định rõ *Bên Kiểm soát dữ liệu* (Data Controller – quyết định mục đích, phương tiện xử lý) [20] ; *Bên Xử lý dữ liệu* (Data Processor – xử lý thay mặt controller theo hợp đồng) [21] ; *Bên Kiểm soát và Xử lý* (tự thu thập và trực tiếp xử lý – tương tự mô hình kết hợp) [22] ; và *Bên thứ ba* (nhận dữ liệu từ controller/ processor theo quy định pháp luật hoặc sự đồng ý của chủ thể) [23] . – **Hợp đồng xử lý dữ liệu:** Bắt buộc phải có khi một bên chuyển dữ liệu cho bên khác xử lý. *Bên Xử lý chỉ được tiếp nhận dữ liệu cá nhân sau khi có hợp đồng hoặc thỏa thuận với bên Kiểm soát* [24] ; phải **xử lý đúng mục**	**Cloud khách hàng (tổ chức sử dụng dịch vụ):** Phải tuân thủ chặt chẽ các quy định bảo vệ dữ liệu cá nhân khi đưa dữ liệu lên cloud, đặc biệt nếu dữ liệu đó là của cá nhân người VN. Cụ thể: – **Thu thập và sử dụng đúng mục đích, phạm vi đã thông báo & được consent:** Trước khi đưa dữ liệu cá nhân lên cloud (nhất là cloud nước ngoài), cần bảo đảm đã có sự đồng ý của chủ thể dữ liệu, bao gồm việc chủ thể đã biết dữ liệu có thể được lưu trữ/xử lý qua bên thứ ba (CSP) và thậm chí chuyển ra ngoài lãnh thổ VN. Việc	NĐ 13/2023/NĐ-CP, Điều 1-2 [12] [43] ; Điều 2.9-2.11 [20] [21] ; Điều 22-25 [29] [30] ; Điều 39 [24] [27] .

	tin trẻ em <16 tuổi...) [13] [14] . – **Nguyên tắc xử lý DLCN:** Phải có căn cứ pháp lý (thông thường là **sự đồng ý** của chủ thể dữ liệu trừ các trường hợp ngoại lệ), xử lý đúng mục đích đã thông báo, **chỉ thu thập trong phạm vi cần thiết**, đảm bảo an toàn, bảo mật dữ liệu, và **chứng minh được sự tuân thủ** các nguyên tắc này [15] [16] . – **Quyền của chủ thể dữ liệu:** Biết, đồng ý hoặc không đồng ý, truy cập, rút consent, xóa, hạn chế xử lý, cung cấp dữ liệu của mình... (với một số ngoại lệ luật định) [17] [18] . – **Nghĩa vụ của bên xử**	**đích, phạm vi trong hợp đồng** [25] ; đồng thời **áp dụng đầy đủ biện pháp bảo vệ dữ liệu cá nhân** theo NĐ 13 và pháp luật liên quan [26] . Sau khi hoàn thành, **phải xóa hoặc trả lại toàn bộ DLCN cho bên Kiểm soát** [27] . Bên xử lý cũng **chịu trách nhiệm trước chủ thể dữ liệu về thiệt hại xảy ra** do quá trình xử lý của mình [28] . – **Chuyển dữ liệu cá nhân ra nước ngoài:** Có **yêu cầu đặc thù**. Điều 25 quy định *DLCN công dân VN chỉ được phép chuyển ra nước ngoài* **khi bên chuyển dữ liệu lập "Hồ sơ đánh giá tác động" (DPIA)** và **thực hiện thủ tục gửi hồ sơ, thông báo tới Bộ Công an** theo	đồng ý phải được thể hiện bằng định dạng lưu trữ được (văn bản hoặc điện tử) [38] và chủ thể phải biết rõ nội dung dữ liệu, mục đích, bên sẽ xử lý... [39] [40] . – **Hạn chế chuyển dữ liệu cá nhân ra nước ngoài khi chưa làm DPIA:** Nếu tổ chức dự định sử dụng cloud đặt máy chủ ở nước ngoài (ví dụ thuê vùng AWS Singapore để lưu thông tin cá nhân khách hàng), **bắt buộc phải lập Hồ sơ Đánh giá tác động và gửi Bộ Công an** theo NĐ 13 [29] [30] . Đây là thủ tục mới, đòi hỏi doanh nghiệp chuẩn bị phân tích chi

		lý dữ liệu: Bảo đảm thực hiện các quyền của chủ thể; bảo mật dữ liệu; xóa dữ liệu theo yêu cầu; thông báo khi có vi phạm; **không được cung cấp hay bán dữ liệu cá nhân khi chưa có sự đồng ý** (trừ trường hợp pháp luật cho phép) [19] .	quy định [29] [30] . Hồ sơ DPIA phải chứa các thông tin chi tiết về bên chuyển, bên nhận, mục đích chuyển, loại dữ liệu chuyển, biện pháp bảo vệ, đánh giá rủi ro, có cam kết ràng buộc trách nhiệm giữa bên chuyển – bên nhận… [31] [32] . Bên chuyển phải **luôn lưu giữ hồ sơ DPIA và sẵn sàng cho Bộ CA kiểm tra**; đồng thời **gửi 01 bản chính hồ sơ cho Bộ CA (Cục A05)** trong vòng 60 ngày kể từ khi bắt đầu chuyển dữ liệu [30] . Sau khi chuyển xong phải **thông báo bằng văn bản** cho Bộ CA về việc đã chuyển thành công và cung cấp thông tin liên hệ của người phụ trách dữ liệu ở bên nhận [33] .	tiết mục đích, loại dữ liệu, biện pháp bảo vệ và đánh giá rủi ro khi đưa dữ liệu ra nước ngoài. Nếu chưa thực hiện, **việc chuyển dữ liệu cá nhân ra nước ngoài là vi phạm** (có thể bị yêu cầu dừng ngay việc chuyển). Trong hồ sơ DPIA cần **nêu rõ biện pháp bảo vệ áp dụng**, do đó doanh nghiệp nên triển khai các biện pháp như **mã hóa dữ liệu, ẩn danh hóa** trước khi lưu trên cloud nước ngoài để giảm rủi ro và đưa vào hồ sơ như biện pháp bảo vệ [32] . – **Quản lý chặt chẽ bên Xử lý dữ liệu (CSP):** Khi

		Bộ CA sẽ **đánh giá hồ sơ**, nếu chưa đầy đủ đúng quy định có thể yêu cầu bên chuyển **hoàn thiện** bổ sung [34]. – **Kiểm soát chuyển dữ liệu & xử lý vi phạm:** Bộ CA được quyền **kiểm tra hoạt động chuyển dữ liệu ra nước ngoài 1 lần/ năm** (trừ khi có dấu hiệu vi phạm sẽ kiểm tra đột xuất) [35]. Bộ CA có thể **yêu cầu ngừng chuyển dữ liệu** nếu phát hiện dữ liệu chuyển ra bị sử dụng xâm hại an ninh quốc gia, hoặc bên chuyển **không tuân thủ quy định gửi/hoàn thiện hồ sơ DPIA**, hoặc **để xảy ra sự cố lộ, mất dữ liệu cá nhân công dân VN** [36] [37].	thuê dịch vụ cloud, tổ chức đóng vai trò "Bên Kiểm soát dữ liệu" và CSP là "Bên Xử lý dữ liệu". NĐ 13 yêu cầu phải ký **hợp đồng hoặc thỏa thuận bằng văn bản về xử lý dữ liệu** trước khi chuyển dữ liệu cho CSP [24]. Hợp đồng này (DPA) cần quy định rõ phạm vi, mục đích xử lý; các tiêu chuẩn bảo mật CSP phải đáp ứng; cam kết chỉ xử lý theo chỉ đạo của khách hàng; không được sử dụng dữ liệu cho mục đích khác; và **nghĩa vụ xóa/ trả lại dữ liệu khi chấm dứt** [27]. Nếu CSP thuê lại hạ tầng hay dùng bên thứ ba (sub-processor),

		cần có điều khoản buộc CSP **đảm bảo bên thứ ba cũng tuân thủ tương đương**. Ngoài ra, tổ chức cần đánh giá năng lực bảo mật của CSP (ví dụ chứng chỉ ISO 27001, PCI-DSS, báo cáo SOC2...) để đáp ứng yêu cầu "có biện pháp bảo vệ phù hợp" [26]. – **Thông báo vi phạm và phối hợp với Bộ CA:** NĐ 13 yêu cầu các tổ chức, cá nhân liên quan có trách nhiệm **thông báo kịp thời cho Bộ Công an** về các vi phạm liên quan đến bảo vệ dữ liệu cá nhân [41]. Do đó, nếu xảy ra sự cố lộ lọt dữ liệu trên cloud, khách hàng cần

		báo cáo sớm cho Cục A05. Đồng thời, hợp đồng với CSP nên có điều khoản yêu cầu CSP **thông báo sự cố cho khách hàng ngay** khi phát hiện để khách hàng thực hiện nghĩa vụ này. **Cloud của CSP (nhà cung cấp dịch vụ):** CSP hoạt động tại VN (kể cả nước ngoài có chi nhánh) cũng chịu các nghĩa vụ của bên xử lý dữ liệu: – **Chỉ được xử lý dữ liệu theo hợp đồng với khách hàng**, không tự ý thu thập thêm hay dùng dữ liệu cho mục đích khác [25]. – **Áp dụng đầy đủ biện pháp bảo vệ**

Văn bản	Cơ quan ban hành	Phạm vi áp dụng	Quy định liên quan đến cloud/ data	Nghĩa vụ chính	Ảnh hưởng đối với cloud nước ngoài vs. nội địa	Nguồn
					dữ liệu cá nhân: triển khai kiểm soát truy cập, mã hóa, phòng chống rò rỉ... theo tiêu chuẩn tốt để đảm bảo an toàn cho dữ liệu khách hàng [26]. – **Xóa, trả dữ liệu khi kết thúc hợp đồng:** CSP phải có quy trình xóa dữ liệu triệt để khỏi hệ thống khi khách hàng yêu cầu hoặc khi chấm dứt dịch vụ [27]. – **Hợp tác với cơ quan có thẩm quyền:** cung cấp thông tin phục vụ điều tra các vi phạm về dữ liệu cá nhân theo yêu cầu của Bộ CA [42].	

Luật An toàn Thông tin mạng 2015 (số 86/2015/QH13, hiệu lực 01/7/2016) và **Nghị định 85/2016/NĐ-CP** về đảm bảo an toàn hệ thống thông tin theo cấp độ	Quốc hội; Chính phủ	Luật ATTTM 2015 điều chỉnh hoạt động bảo đảm an toàn thông tin mạng (bao gồm bảo vệ dữ liệu, hệ thống, ứng dụng) cho mọi cơ quan, tổ chức, cá nhân. Nghị định 85/2016 triển khai chi tiết *đối với hệ thống thông tin của CQNN và dịch vụ công*, đồng thời **khuyến khích tổ chức, cá nhân khác áp dụng** [44].	– **Phân loại mức độ an toàn hệ thống thông tin (HTTT):** NĐ 85 đưa ra **5 cấp độ** cho HTTT, từ cấp 1 (thấp nhất) đến cấp 5 (cao nhất), dựa trên mức độ quan trọng của thông tin được xử lý và **hậu quả nếu hệ thống bị xâm phạm** [45] [46]. Ví dụ: *cấp độ 1* là hệ thống phục vụ hoạt động nội bộ, chỉ chứa thông tin công cộng [47] [48]; *cấp độ 5* là hệ thống có thông tin tuyệt mật, sống còn đối với ANQG. – **Tiêu chí phân loại:** Thông tin được phân loại theo **thuộc tính bí mật** (công cộng, riêng tư, bí mật cá nhân,	– **Đối với tổ chức sử dụng cloud:** Cần **xác định cấp độ an toàn** cho hệ thống thông tin mà mình đưa lên cloud. Ví dụ, một ứng dụng phục vụ người dân (dịch vụ công trực tuyến) có thể được phân loại cấp 3; một hệ thống nội bộ trường học có thể cấp 2. Khi thuê cloud, tổ chức phải đảm bảo **CSP đáp ứng được yêu cầu kỹ thuật tương ứng cấp độ**. Điều này có nghĩa: nếu hệ thống ở cấp 3+, CSP phải có các biện pháp bảo mật nâng cao (quản trị phân quyền chặt, giám sát 24/7, phương án dự phòng thảm họa, thiết bị an ninh chuyên dụng...). Nếu CSP không đáp ứng, tổ chức **không nên đưa hệ thống đó lên cloud công**	Luật ATTTM 2015; NĐ 85/2016/NĐ-CP [53] [52]; TT 12/2022/TT-BTTTT.

	bí mật NN) và **theo chức năng hệ thống** (nội bộ, dịch vụ cung cấp cho dân/ doanh nghiệp, hạ tầng thông tin quan trọng, hệ thống điều khiển công nghiệp...) [49]. Mỗi cấp độ có tiêu chí riêng; từ cấp 1 đến 5 yêu cầu tăng dần về phạm vi ảnh hưởng và độ mật của thông tin [47]. – **Thẩm quyền phê duyệt cấp độ:** Đối với hệ thống của cơ quan nhà nước: cấp 1-2 do đơn vị chuyên trách ATTT của cơ quan tự thẩm định phê duyệt; cấp 3 do đơn vị chuyên trách ATTT thẩm định và người đứng đầu cơ quan phê	**cộng**. – **Cloud cho cơ quan nhà nước:** Hiện nay Bộ TT&TT đã ban hành **Thông tư 12/2022/TT-BTTTT** (thay thế Thông tư 03/2017) hướng dẫn chi tiết NĐ 85, đặt ra **bộ tiêu chí kỹ thuật cho từng cấp độ**. Các CSP muốn cung cấp dịch vụ cho cơ quan nhà nước thường phải **đạt chứng nhận phù hợp cấp độ 3 hoặc 4** (tùy dữ liệu). Do đó, CSP trong nước thường công bố khả năng đáp ứng cấp độ (VD: chứng nhận đảm bảo ATTT cấp độ 3 cho hệ thống chính phủ). – **Dịch vụ cloud xuyên biên giới:** NĐ 85 không cấm đặt hệ thống cấp thấp trên cloud nước ngoài, nhưng nếu là **thông tin quan trọng (cấp**

	duyệt; cấp 4-5 phải gửi hồ sơ đề xuất lên Bộ CA hoặc Bộ QP (theo lĩnh vực) hoặc Bộ TT&TT thẩm định, sau đó *chủ quản hệ thống* phê duyệt cấp 4 (kèm phương án bảo đảm ATTT cấp 5) và Thủ tướng phê duyệt danh mục hệ thống cấp 5 [50] [51]. (Nói cách khác, hệ thống quan trọng cấp quốc gia cần sự chấp thuận ở tầm quốc gia). – **Yêu cầu đảm bảo an toàn theo cấp độ:** Với mỗi cấp độ, hệ thống phải đáp ứng **các yêu cầu cơ bản về kỹ thuật và quản lý** tương ứng. NĐ 85 yêu cầu xây dựng **phương án**	**4-5, như dữ liệu chính phủ quan trọng, hạ tầng quốc gia)** thì **không phù hợp để đưa ra ngoài lãnh thổ** do yêu cầu bảo mật rất cao. Ngay cả với cấp 3 (như dữ liệu cá nhân nhiều người, dịch vụ công), việc lưu trữ trên cloud nước ngoài có thể khiến cơ quan QLNN e ngại về **khả năng kiểm soát**. Vì vậy trên thực tế, **các hệ thống chính phủ, ngành tài chính, y tế quan trọng đều ưu tiên cloud nội địa** hoặc private cloud. – **Tuân thủ ATTT liên tục:** Sử dụng cloud không miễn trừ trách nhiệm tuân thủ ATTT. Tổ chức vẫn phải **duy trì kiểm tra đánh giá định kỳ** cho hệ thống của mình trên

	bảo đảm ATTT cho hệ thống, gồm các nội dung: an toàn trong thiết kế, xây dựng, vận hành; giám sát, đánh giá, quản lý rủi ro; phương án dự phòng, ứng cứu sự cố và khôi phục; và phương án khi kết thúc, thanh lý hệ thống [52]. Các phương án này phải **tuân thủ tiêu chuẩn, quy chuẩn kỹ thuật về ATTT theo cấp độ** do cơ quan QLNN ban hành [52]. (Ví dụ: có bộ tiêu chuẩn kỹ thuật chi tiết cho từng cấp). – **Kiểm tra, đánh giá:** Hệ thống từ cấp 3 trở lên thường phải **kiểm tra, đánh giá ATTT định kỳ** (thường hàng năm)	cloud. Nếu hệ thống trên cloud xảy ra sự cố nghiêm trọng, tổ chức có thể bị cơ quan quản lý kiểm tra việc tuân thủ phương án ATTT đã phê duyệt.

Văn bản	Cơ quan ban hành	Phạm vi áp dụng	Quy định liên quan đến cloud/ data	Nghĩa vụ chính	Ảnh hưởng đối với cloud nước ngoài vs. nội địa	Nguồn
			và trước khi đưa vào vận hành. Các hệ thống cấp độ cao (4,5) có thể đòi hỏi **kiểm tra độc lập** bởi cơ quan chuyên trách hoặc tổ chức đánh giá được chỉ định.			

Luật Bảo vệ Bí mật Nhà nước 2018 (số 29/2018/QH14, hiệu lực 01/7/2020) và **Nghị định 26/2020/NĐ-CP** hướng dẫn	Quốc hội; Chính phủ	Áp dụng cho mọi cơ quan, tổ chức, cá nhân có hoạt động **bảo vệ bí mật nhà nước (BMNN)**. Luật định nghĩa BMNN là thông tin có nội dung quan trọng về chính trị, quốc phòng, an ninh, ngoại giao… mà **Nhà nước không công bố, nếu lộ sẽ gây nguy hại đến quốc gia**. Danh mục BMNN cụ thể do Thủ tướng ban hành cho từng ngành/lĩnh vực.	– **Phân loại độ mật:** BMNN chia thành 3 độ: **Tuyệt mật, Tối mật, Mật**. Mỗi độ mật có thời hạn bảo vệ (Tuyệt mật 30 năm, Tối mật 20 năm, Mật 10 năm, trừ khi gia hạn) [54] [55] . – **Nguyên tắc bảo vệ:** BMNN phải được quản lý chặt chẽ, **chỉ những người có trách nhiệm mới được tiếp cận**; sao chụp, chuyển giao BMNN phải đúng quy định. **Phương tiện, thiết bị lưu trữ BMNN** phải đảm bảo an ninh (ví dụ: tài liệu giấy khóa tủ, tài liệu số phải mã hóa, lưu trên hệ thống biệt lập…). – **Hành vi bị nghiêm cấm:** Tiết lộ,	– **Dữ liệu "nhạy cảm" trong tổ chức:** Nếu tổ chức có dữ liệu thuộc danh mục BMNN (VD: một trường ĐH quốc phòng có tài liệu nghiên cứu quốc phòng cấp mật), **tuyệt đối không được đưa lên public cloud**. Việc **đưa BMNN lên hạ tầng cloud nước ngoài** có thể bị xem là "truyền đưa BMNN trái phép ra nước ngoài", vi phạm nghiêm trọng luật BMNN [56] . Ngay cả lưu trên cloud nội địa cũng đòi hỏi **cloud đó phải đủ điều kiện bảo mật** (ví dụ phải là mạng nội bộ dùng thiết bị mã hóa được cấp phép). Thông thường, BMNN chỉ lưu trong hệ thống riêng, không nối	Luật BMNN 2018 [58] [59] ; NĐ 26/2020/NĐ-CP.

	chiếm đoạt, mua bán BMNN; **lưu giữ, truyền đưa BMNN trái phép trên mạng viễn thông, internet**; làm lộ BMNN do sơ suất… (Điều 5 Luật) [56] [57] . – **Nghĩa vụ cơ quan, tổ chức:** Phải **xác định cụ thể thông tin thuộc BMNN trong phạm vi mình**, thực hiện **đóng dấu, phân cấp độ mật** cho tài liệu, và **bảo quản theo chế độ mật**. Khi **chuyển giao BMNN** (kể cả gửi email hay lưu trữ điện tử) phải sử dụng **phương tiện mã hóa do cơ quan chuyên trách quy định** (thường là hệ thống do Ban Cơ yếu	Internet. – **Phân biệt BMNN với dữ liệu nhạy cảm khác:** Chỉ những thông tin nằm trong *danh mục BMNN do nhà nước quy định* mới thuộc phạm vi luật này. Các dữ liệu nhạy cảm doanh nghiệp (bí mật kinh doanh, tài chính nội bộ…) **không phải BMNN**, mà thuộc phạm vi bảo mật thông tin thông thường. Doanh nghiệp có thể lưu bí mật kinh doanh trên cloud nhưng nên mã hóa và kiểm soát chặt truy cập. – **Trách nhiệm cá nhân:** Người sử dụng dịch vụ cloud phải được quán triệt: **nếu vô ý làm lộ thông tin thuộc BMNN (ví dụ upload tài liệu mật lên cloud public rồi bị truy cập**

Văn bản	Cơ quan ban hành	Phạm vi áp dụng	Quy định liên quan đến cloud/ data	Nghĩa vụ chính	Ảnh hưởng đối với cloud nước ngoài vs. nội địa	Nguồn
				trái phép), cá nhân đó có thể bị xử lý hình sự. Vì vậy tổ chức cần **quy định rõ loại thông tin nào cấm đưa lên cloud** (VD: tài liệu có đóng dấu mật). – **Đối với CSP:** Nếu vô tình lưu trữ dữ liệu BMNN của khách hàng trên hệ thống mình, CSP cần tuân thủ yêu cầu của cơ quan NN khi được yêu cầu thu hồi hoặc xóa thông tin đó. CSP cũng nên có cơ chế cho khách hàng **tự quản lý khóa mã hóa (HYOK)** để ngay cả CSP không thể đọc dữ liệu – giảm nguy cơ vi phạm luật BMNN nếu có dữ liệu nhạy cảm.		
			Chính phủ cấp).			

Văn bản, tiêu chuẩn chuyên ngành về dịch vụ Cloud: - *Hướng dẫn của Bộ TT&TT và các cơ quan quản lý*	Bộ TT&TT; Ngân hàng NN; Bộ GD&ĐT…	Một số lĩnh vực có hướng dẫn hoặc tiêu chuẩn riêng về ứng dụng điện toán đám mây: **(a) Chính phủ điện tử:** Bộ TT&TT ban hành **Công văn 1145/ BTTTT-CATTT (3/4/2020)** hướng dẫn **bộ tiêu chí kỹ thuật lựa chọn nền tảng cloud** phục vụ Chính phủ điện tử. Tiêu chí này đòi hỏi **cloud phải đặt tại VN**, **DC đạt chuẩn Tier 3**, **chứng chỉ an toàn thông tin như ISO 27001, ISO 27017 (cloud security), ISO 27018 (bảo vệ dữ liệu cá**	– **Điều kiện cho CSP muốn phục vụ chính phủ:** CSP cần đạt các tiêu chí kỹ thuật theo hướng dẫn 1145 – ví dụ: phải có **hạ tầng DC tại VN**, được chứng nhận an toàn (ISO 27001, etc.), có năng lực tách biệt vùng dữ liệu cho cơ quan NN, hỗ trợ xác thực, mã hóa theo yêu cầu. Một số CSP Việt Nam như Viettel, VNPT đã công bố đáp ứng các tiêu chí này [60]. – **Tổ chức tài chính – ngân hàng:** Ngân hàng Nhà nước VN ban hành **Thông tư 09/2020/TT-NHNN** cho phép ngân hàng **sử dụng dịch vụ cloud kể cả cho dữ liệu quan trọng (cấp**	**Cloud nội địa vs. nước ngoài – khuyến nghị bởi CQQL:** Thực hiện chủ trương "ưu tiên cloud nội", các cơ quan nhà nước và một số ngành nhạy cảm có xu hướng lựa chọn **cloud của doanh nghiệp Việt Nam** để lưu trữ dữ liệu quan trọng, nhằm **đảm bảo dữ liệu nằm trong lãnh thổ, dưới pháp luật VN quản lý**. Điều này tạo lợi thế cho CSP nội địa trong lĩnh vực chính phủ, tài chính. Tuy nhiên, với doanh nghiệp tư nhân, việc chọn cloud nước ngoài không bị cấm, miễn tuân thủ các luật chung (ANM, Bảo vệ DL, ATTT…). Doanh nghiệp cần tự đánh giá: nếu dữ liệu thuộc loại phải lưu tại VN (theo Luật

nhân trên cloud), tuân thủ **Tiêu chuẩn quốc gia về TTXVN cấp độ 4**... [60]. **(b) Chuyển đổi số quốc gia:** Quyết định 749/QĐ-TTg (2020) nêu nguyên tắc "Cloud First" – khuyến khích cơ quan nhà nước ưu tiên sử dụng dịch vụ điện toán đám mây do các doanh nghiệp Việt Nam cung cấp để đảm bảo chủ quyền số. **(c) Giáo dục:** Hiện chưa có quy định chuyên biệt về cloud cho giáo dục, nhưng Bộ GD&ĐT	**độ 3-5)**, với điều kiện đảm bảo an toàn [61]. TT 09 đặt ra **tiêu chí chọn CSP**: phải là **doanh nghiệp** (pháp nhân hợp pháp); có **hạ tầng CNTT đáp ứng quy định pháp luật VN**; có **chứng nhận quốc tế về an toàn thông tin còn hiệu lực** (ISO 27001, v.v.) [62]. Hợp đồng với CSP phải bao gồm: dữ liệu phát sinh thuộc sở hữu ngân hàng [62]; khi chấm dứt dịch vụ, **CSP phải trả lại hoặc hỗ trợ chuyển toàn bộ dữ liệu về cho ngân hàng, và cam kết xóa hết dữ liệu của ngân hàng trong thời gian nhất định**; **đảm bảo dữ liệu**	ANM hoặc thỏa thuận với cơ quan NN), thì **không đưa lên cloud nước ngoài**; nếu dữ liệu quan trọng yêu cầu khả năng bảo mật cao, nên cân nhắc cloud nội địa có chứng nhận. **Chuẩn mực quốc tế:** Ngoài tuân thủ luật VN, doanh nghiệp dùng cloud nên tham khảo các tiêu chuẩn quốc tế liên quan (ISO 27017 cho bảo mật cloud, ISO 27701 cho quản lý thông tin cá nhân, PCI-DSS nếu lưu dữ liệu thẻ thanh toán, v.v.). Nhiều CSP lớn đã tuân thủ các tiêu chuẩn này, giúp việc đánh giá an toàn dễ hơn. **Thuế và thương mại điện tử:** Lưu ý, thuê dịch vụ cloud nước ngoài có thể phát sinh **thuế nhà thầu**; và

	khuyến nghị các cơ sở giáo dục chuyển đổi số, sử dụng cloud để triển khai các hệ thống quản lý, học trực tuyến. Ưu tiên nền tảng trong nước cho dữ liệu học sinh, sinh viên.	**ngân hàng tách biệt với dữ liệu khách hàng khác trên cùng hệ thống** [63]. Ngoài ra ngân hàng phải **đánh giá rủi ro trước khi dùng cloud** và gửi báo cáo NHNN [64]; đánh giá tuân thủ của CSP hàng năm; xây dựng phương án dự phòng khi dùng cloud nước ngoài (đảm bảo hoạt động liên tục nếu mất kết nối quốc tế) [65]. – **Y tế:** Bộ Y tế chưa có quy định riêng về cloud, nhưng dữ liệu y tế (hồ sơ bệnh án, thông tin sức khỏe) thuộc loại **DLCN nhạy cảm** theo NĐ 13 [66], do đó các bệnh viện khi dùng	CSP nước ngoài cung cấp dịch vụ số tại VN phải đăng ký thuế và nộp thuế GTGT theo quy định (VD: Google, AWS đã đăng ký). Doanh nghiệp cần kiểm tra nhà cung cấp đã tuân thủ nghĩa vụ thuế để tránh rủi ro gián đoạn dịch vụ do vấn đề pháp lý.

	cloud phải đặc biệt bảo mật và thường ưu tiên cloud đặt tại VN, tuân thủ quy định bảo mật ngành y (VD: Thông tư 54/2017/TT-BYT về bảo mật hệ thống CNTT y tế). – **Giáo dục:** Dữ liệu giáo dục gồm thông tin học sinh, giáo viên, kết quả học tập... phần lớn là **dữ liệu cá nhân cơ bản** (tên, ngày sinh, điểm số) nhưng cũng có thể bao hàm dữ liệu nhạy cảm (ví dụ thông tin sức khỏe tâm lý của học sinh). Các trường học, EdTech khi dùng cloud phải tuân thủ NĐ 13 về bảo vệ dữ liệu học sinh (nếu học sinh <16 tuổi, cần có sự đồng ý

Văn bản	Cơ quan ban hành	Phạm vi áp dụng	Quy định liên quan đến cloud/ data	Nghĩa vụ chính	Ảnh hưởng đối với cloud nước ngoài vs. nội địa	Nguồn
			của cha mẹ theo Luật Trẻ em 2016). Nên lựa chọn CSP có cam kết bảo vệ dữ liệu trẻ em. Tại VN, nhiều trường đã dùng dịch vụ cloud của các hãng lớn (Google Workspace, Microsoft 365) – các dịch vụ này lưu trữ dữ liệu ngoài lãnh thổ nên **cần đánh giá tác động và đăng ký với Bộ CA** tương tự yêu cầu NĐ 13, đồng thời nhà trường phải thông báo phụ huynh, học sinh về việc dữ liệu được lưu trên hệ thống nước ngoài.			

Chú thích: Bên cạnh các văn bản trên, doanh nghiệp có thể cần tuân thủ thêm các luật chung khác như **Luật Viễn thông sửa đổi 2023**, **Luật Giao dịch điện tử 2023**, **Luật Công nghệ thông tin 2006** (đang được

dự thảo sửa đổi) – các luật này quy định về điều kiện kinh doanh và tính pháp lý của dịch vụ CNTT, nhưng nội dung chi tiết liên quan cloud sẽ được đề cập ở phần sau (nhất là Luật Viễn thông 2023 đối với CSP).

B) Sử dụng Public Cloud nước ngoài – "Decision Tree" pháp lý

Một trong những mối quan tâm lớn là **khả năng sử dụng dịch vụ cloud đặt máy chủ ở nước ngoài** (ví dụ các region cloud quốc tế) trong khuôn khổ pháp luật Việt Nam. Dưới đây là **hướng dẫn theo dạng cây quyết định** giúp tổ chức xác định trường hợp nào **được phép**, **điều kiện kèm theo**, khi nào cần **lưu dữ liệu trong nước hoặc xin phép trước khi chuyển dữ liệu**, và trường hợp nào **rủi ro cao, không khuyến nghị** vì xung đột pháp lý.

Bảng: Quyết định sử dụng Public Cloud (đặt máy chủ ở nước ngoài)

1. Dữ liệu có thuộc loại *phải lưu trữ tại Việt Nam* theo luật? *Ví dụ:* Dữ liệu thuộc danh mục Điều 26 Luật ANM (thông tin cá nhân người dùng VN, dữ liệu người dùng tạo ra) đối với doanh nghiệp cung cấp dịch vụ internet; hoặc dữ liệu cá nhân khách hàng NH giai đoạn 2018-2020 theo TT 18/2018 NHNN; hoặc dữ liệu mật nhà nước…	– Dữ liệu rơi vào quy định **bắt buộc lưu trữ tại VN** theo luật chuyên ngành hoặc an ninh quốc gia (VD: dữ liệu người dùng VN nếu DN thuộc diện Điều 26 Luật ANM; dữ liệu khách hàng NH trước 2020…) [1] [65] . – Hoặc dữ liệu thuộc loại **cấm đưa ra nước ngoài** (VD: bí mật nhà nước, thông tin an ninh quan trọng cấp độ 5).	**Không được sử dụng public cloud nước ngoài** (Not Allowed). **Khuyến nghị:** Sử dụng **cloud nội địa hoặc hệ thống CNTT nội bộ** để lưu trữ các dữ liệu này, tuân thủ đúng yêu cầu pháp luật. Có thể dùng giải pháp hybrid (dữ liệu nhạy cảm giữ trong nước, chỉ đưa dữ liệu ít quan trọng lên cloud ngoài).	– Nếu buộc phải sử dụng dịch vụ nước ngoài (do không có lựa chọn tương đương trong nước), cần **xin ý kiến cơ quan quản lý chuyên ngành**. Tuy nhiên, thông thường pháp luật đã cấm hoặc hạn chế rõ (ví dụ BMNN cấm lưu trên hạ tầng không được phép). – *Trường hợp Luật ANM:* Nếu DN vẫn muốn phục vụ người dùng VN bằng hạ tầng ngoài, phải chấp nhận **khả năng nhận yêu cầu từ Bộ CA** yêu cầu lưu bản trong nước + đặt VPĐD. Lúc đó **phải thực hiện trong 12 tháng** [6] .	– **Kiểm soát thay thế:** Nếu không thể đưa dữ liệu ra ngoài, triển khai giải pháp trong nước: mã hóa toàn bộ dữ liệu, phân vùng mạng chặt chẽ, hạn chế truy cập remote. Đối với BMNN, sử dụng thiết bị **mã hóa được cấp phép** khi lưu trữ, truyền tải. – **Giám sát tuân thủ:** Thiết lập cơ chế kiểm tra định kỳ đảm bảo dữ liệu này **không vô tình bị đồng bộ ra dịch vụ cloud nước ngoài** (VD: không để nhân viên tải tài liệu mật lên Google Drive cá nhân).	– **Rủi ro pháp lý:** Vi phạm rõ ràng quy định nội địa hóa hoặc bảo vệ BMNN, có thể dẫn đến **xử phạt nặng, đình chỉ dịch vụ, truy cứu trách nhiệm**. – **Rủi ro an ninh:** Dữ liệu nhạy cảm lọt ra hạ tầng nước ngoài có nguy cơ **bị truy cập bởi chính phủ nước khác** theo luật của họ, hoặc bị lộ do CSP nước ngoài không chịu sự kiểm soát của VN. – **Khả năng cưỡng chế:** Nếu tổ chức cố tình dùng cloud nước ngoài cho dữ liệu bị hạn chế, cơ quan VN có thể yêu cầu **xóa hoặc thu hồi dữ liệu**. Nếu CSP không tuân thủ (do ở ngoài thẩm quyền), tổ chức sẽ **mắc kẹt** giữa nghĩa vụ pháp

Bước quyết định	Điều kiện/ Loại dữ liệu	Kết luận sử dụng	Thủ tục/Hồ sơ yêu cầu trước khi chuyển	Kiểm soát tối thiểu cần áp dụng	Rủi ro còn lại
					lý và hợp đồng với CSP.

2. Dữ liệu có chứa thông tin cá nhân của công dân Việt Nam? (*Bao gồm cả dữ liệu khách hàng, nhân viên, học sinh/ sinh viên VN, email, tên, số điện thoại, v.v.*)	– Dữ liệu bao gồm **thông tin nhận dạng cá nhân** (PII) của người VN – theo định nghĩa NĐ 13/2023. Bao gồm cả dữ liệu cá nhân nhạy cảm (sức khỏe, tài chính, trẻ em, v.v.) [13] . – Dữ liệu này chưa có quy định bắt buộc lưu nội địa, nhưng chịu sự điều chỉnh của **NĐ 13 về bảo vệ DLCN**.	**Có thể sử dụng public cloud nước ngoài** một cách **Có điều kiện** (Allowed *with conditions*). Luật không cấm lưu dữ liệu cá nhân ở nước ngoài, **nhưng yêu cầu nhiều thủ tục bảo vệ trước và trong khi chuyển**. Nếu đáp ứng các điều kiện dưới đây, việc sử dụng là hợp pháp.	**Trước khi chuyển dữ liệu:** – **Lập Hồ sơ Đánh giá Tác động chuyển dữ liệu (DTIA)** theo Điều 25 NĐ 13 [29] . Hồ sơ này phân tích mục đích, loại dữ liệu, bên nhận, biện pháp bảo vệ, rủi ro... khi đưa dữ liệu cá nhân ra ngoài. – **Gửi 01 bản hồ sơ DTIA cho Bộ Công an (Cục A05)** trong vòng 60 ngày từ khi bắt đầu chuyển dữ liệu [30] . Không cần chờ phê duyệt, nhưng Bộ CA có thể xem xét và yêu cầu bổ sung nếu chưa đạt [34] . – **Thông báo bằng văn bản cho Bộ CA sau khi chuyển thành công**	**Trong khi sử dụng cloud nước ngoài:** – **Ký Thỏa thuận/Hợp đồng xử lý DL với CSP** (Data Processing Agreement): Ràng buộc CSP chỉ xử lý dữ liệu theo mục đích cho phép, bảo mật, không tiết lộ cho bên thứ ba nếu chưa được đồng ý [25] [42] . Đặc biệt, yêu cầu CSP **xóa dữ liệu ngay khi có yêu cầu hoặc khi kết thúc hợp đồng** [27] . – **Áp dụng các biện pháp bảo vệ kỹ thuật**: Mã hóa dữ liệu cá nhân nhạy cảm trước khi lưu (nên dùng giải pháp **mã hóa đầu cuối, BYOK/HYOK** để CSP không giữ khóa); Ẩn danh hoặc pseudonymize dữ liệu nếu có thể; Bật logging giám sát truy cập (để phát hiện truy cập trái phép). – **Hạn chế phạm vi dữ liệu đưa ra**: Chỉ chuyển ra ngoài những dữ liệu thật sự cần thiết cho mục đích đã định. Dữ liệu không cần thiết nên **lưu trên hệ thống trong nước**. – **Đảm**	– **Rủi ro vi phạm nếu thiếu thủ tục**: Nếu không thực hiện DPIA và gửi Bộ CA, việc chuyển dữ liệu cá nhân ra ngoài là **không tuân thủ NĐ 13**, có thể bị yêu cầu dừng chuyển dữ liệu và xử phạt (dù hiện nay chế tài NĐ 13 chưa rõ, rủi ro chính là bị buộc **ngừng sử dụng cloud nước ngoài** cho dữ liệu đó) [36] . – **Rủi ro bảo mật**: Dữ liệu cá nhân trên cloud nước ngoài có nguy cơ bị truy cập bởi bên thứ ba hoặc cơ quan nước ngoài theo pháp luật nơi đặt máy chủ (vd cơ quan thực thi pháp luật nước sở tại). Mã hóa mạnh giúp giảm rủi ro này, nhưng nếu CSP nước ngoài bị yêu cầu (theo MLAT chẳng

Bước quyết định	Điều kiện/ Loại dữ liệu	Kết luận sử dụng	Thủ tục/Hồ sơ yêu cầu trước khi chuyển	Kiểm soát tối thiểu cần áp dụng	Rủi ro còn lại
			(gồm thông tin liên hệ người phụ trách ở nước ngoài) [33]. *(Các thủ tục này hiện không thu phí nhưng đòi hỏi công phu chuẩn bị)*.	**bảo quyền của chủ thể dữ liệu**: Thiết lập quy trình cho phép chủ thể dữ liệu VN thực hiện quyền (yêu cầu xóa, chỉnh sửa, rút consent). CSP phải hỗ trợ đáp ứng trong 72 giờ nếu xóa/hạn chế, trừ trường hợp pháp luật khác cho phép chậm hơn [67] [68].	hạn), dữ liệu có thể bị giải mã nếu họ có khóa. – **Khó khăn trong thực thi quyền chủ thể**: Nếu CSP không hợp tác hoặc không có cơ chế hỗ trợ xóa dữ liệu theo yêu cầu, tổ chức sẽ **khó tuân thủ** quyền xóa/ hạn chế trong 72 giờ như luật định [67]. – **Kiểm soát sau chuyển**: Bộ CA có quyền kiểm tra hàng năm, nếu phát hiện vi phạm hoặc sự cố lộ lọt, có thể yêu cầu ngừng chuyển dữ liệu tiếp [35] [37]. Do đó, tổ chức phải **duy trì tuân thủ liên tục**, cập nhật hồ sơ DPIA khi có thay đổi (VD đổi CSP, chuyển thêm loại dữ liệu mới) [34].

3. Dữ liệu thuộc loại quan trọng, nhạy cảm cao (nhưng không bị luật cấm chuyển)? *Ví dụ:* Dữ liệu tài chính doanh nghiệp, bí mật kinh doanh, dữ liệu khách hàng quan trọng; hệ thống CNTT cấp độ 3-4 (theo NĐ 85) nhưng không thuộc BMNN.	– Dữ liệu có **tầm quan trọng chiến lược** với tổ chức (mất hoặc lộ sẽ gây thiệt hại lớn tài chính, uy tín) – ví dụ CSDL khách hàng VIP, mã nguồn phần mềm độc quyền. – Dữ liệu có thể chứa **bí mật kinh doanh** (không thuộc BMNN, nhưng quan trọng với cạnh tranh). – Hệ thống thông tin phục vụ dịch vụ công cộng quan trọng (cấp 3 hoặc 4 theo phân loại ATTT), tuy luật không cấm cloud nước ngoài nhưng rủi ro cao nếu gián đoạn.	**Được sử dụng cloud nước ngoài trong một số trường hợp, nhưng không khuyến nghị** trừ khi đáp ứng điều kiện nghiêm ngặt (*Conditional/ High Risk*). Tốt nhất: **Xem xét kiến trúc Hybrid hoặc Multi-cloud** để giảm thiểu phụ thuộc.	**– Thông báo và xin ý kiến cổ đông/cơ quan chủ quản** (nếu có): Đối với dữ liệu trọng yếu doanh nghiệp, việc đưa lên hạ tầng nước ngoài có thể cần được phê duyệt ở cấp cao (HĐQT, hoặc cơ quan chủ quản nếu là tổ chức NN) để đảm bảo đồng thuận về rủi ro. – **Lập phương án dự phòng dữ liệu trong nước**: Luôn duy trì một **bản sao dữ liệu cập nhật trong hệ thống lưu trữ nội bộ hoặc cloud dự phòng tại VN**. Điều này không chỉ đáp ứng một số yêu cầu (VD ngân hàng theo TT 09/2020 phải có phương án đảm bảo	**– Kiểm soát kỹ thuật nâng cao:** • **Mã hóa cấp độ cao**: Sử dụng mã hóa hai lớp (encrypt dữ liệu trước khi đưa lên cloud + cloud tiếp tục mã hóa lúc lưu). Khóa mã hóa do doanh nghiệp giữ (BYOK/HYOK). • **Quản lý truy cập chi tiết:** Áp dụng chính sách **Zero Trust** – mọi truy cập quản trị cloud phải qua xác thực đa yếu tố, các tài khoản admin CSP hỗ trợ phải giám sát. • **Giám sát liên tục:** Thiết lập SIEM giám sát log từ hệ thống cloud, cấu hình cảnh báo bất thường (vd đăng nhập từ quốc gia lạ, tải xuống nhiều dữ liệu). Có thể thuê dịch vụ MDR (Managed Detection & Response) để giám sát 24/7. • **Kiểm toán bảo mật định kỳ:** Thuê bên thứ ba đánh giá bảo mật hệ thống cloud (pentest, config review) hàng năm để phát hiện điểm yếu. – **Kiểm soát hợp đồng:** Yêu cầu bổ sung	**– Rủi ro gián đoạn dịch vụ**: Phụ thuộc vào hạ tầng nước ngoài, nếu đứt cáp, sự cố khu vực thì hệ thống có thể gián đoạn. (Đã từng có trường hợp hệ thống bank trên cloud công cộng bị treo do sự cố AWS khu vực). Kế hoạch DR nội địa giảm rủi ro này nhưng cần thử nghiệm định kỳ. – **Rủi ro pháp lý nước sở tại**: Dữ liệu kinh doanh quan trọng có thể bị tiếp cận qua quy trình pháp lý nước ngoài (ví dụ chính phủ nước nơi đặt server tịch thu server điều tra, dữ liệu doanh nghiệp bị lấy theo diện rộng). Đây là rủi ro khó định lượng. – **Rò rỉ nội bộ CSP**: Trường hợp xấu, nhân viên CSP (ở nước ngoài)

Bước quyết định	Điều kiện/ Loại dữ liệu	Kết luận sử dụng	Thủ tục/Hồ sơ yêu cầu trước khi chuyển	Kiểm soát tối thiểu cần áp dụng	Rủi ro còn lại
			hoạt động liên tục nếu mất kết nối quốc tế [65]) mà còn đảm bảo nếu CSP nước ngoài gặp sự cố, dữ liệu vẫn có sẵn trong nước. – **Đánh giá nhà cung cấp kỹ lưỡng**: Chỉ chọn CSP nước ngoài uy tín, có chứng chỉ bảo mật (ISO 27001, SOC 2) và đã có hiện diện tại VN hoặc khu vực (để hỗ trợ khi cần). Yêu cầu cam kết hợp đồng về vùng lưu trữ (đảm bảo dữ liệu chỉ ở data center đã thỏa thuận, không di chuyển tùy tiện).	điều khoản **bồi thường thiệt hại** nếu CSP vi phạm bảo mật dẫn đến lộ dữ liệu, hoặc vi phạm cam kết uptime gây gián đoạn lớn. Dù CSP lớn thường giới hạn trách nhiệm, việc có thỏa thuận rõ ràng giúp răn đe và tạo cơ sở pháp lý đòi bồi thường khi cần.	có thể truy xuất dữ liệu nếu kiểm soát không chặt. Mã hóa BYOK hạn chế điều này nhưng nếu họ có quyền truy cập hệ thống đang chạy (runtime) thì vẫn tiềm ẩn nguy cơ. – **Tuân thủ địa phương**: Nếu dữ liệu khách hàng nước ngoài lưu ở quốc gia thứ ba, có thể phải tuân thủ luật của quốc gia đó (VD GDPR nếu server ở EU). Điều này tạo thêm gánh nặng tuân thủ đa quốc gia cho doanh nghiệp.

4. Nhà cung cấp cloud có hợp tác đáp ứng yêu cầu pháp lý Việt Nam không? *Đánh giá mức độ "compliance-friendly" của CSP:*	– CSP có **đăng ký hoạt động tại VN** (có MST, nộp thuế) hoặc có **đối tác đại diện** để hỗ trợ các vấn đề pháp lý. – CSP sẵn sàng **ký thỏa thuận tuân thủ địa phương**: ví dụ ký phụ lục DPA theo NĐ 13, chấp nhận sửa một số điều khoản theo luật VN (như cam kết lưu dữ liệu tại VN nếu khách yêu cầu, tuân thủ lệnh cơ quan VN nếu hợp pháp). – CSP cho phép khách hàng **lựa chọn region cụ thể** và cam kết không chuyển dữ liệu ra ngoài	Nếu **CSP hỗ trợ tốt về tuân thủ**, có thể **yên tâm sử dụng** (Allowed) hơn, tất nhiên vẫn cần triển khai các kiểm soát nội bộ. Ngược lại, nếu CSP **không đáp ứng các yêu cầu tối thiểu**, việc sử dụng sẽ **tiềm ẩn rủi ro cao**, **không nên sử dụng cho dữ liệu quan trọng**.	– **Nếu CSP chưa có hiện diện VN**: khách hàng nên yêu cầu CSP **đăng ký nhà thầu và nộp thuế** đúng quy định, tránh rủi ro pháp lý về thuế. – **Nếu CSP từ chối ký phụ lục bảo vệ dữ liệu**: xem xét chuyển sang nhà cung cấp khác thân thiện tuân thủ hơn. – **Làm việc với pháp chế nội bộ**: soạn sẵn các điều khoản cần thiết (theo checklist ở phần D) để đàm phán với CSP. Ghi nhận bằng văn bản các thỏa thuận (email, phụ lục).	– **Kiểm soát thay thế/hạn chế:** Nếu vẫn phải dùng CSP "không thân thiện tuân thủ" (ví dụ dịch vụ độc quyền họ cung cấp), cần **giới hạn loại dữ liệu** đưa lên (chỉ dữ liệu công khai hoặc đã mã hóa); đồng thời **tăng tần suất đánh giá** dịch vụ của họ (tự kiểm tra config, log). – **Kết hợp đa cloud:** Có thể sử dụng **dịch vụ của CSP đó nhưng đi kèm dịch vụ bổ trợ** từ bên thứ ba cho các phần nhạy cảm (VD: dùng AWS tính toán nhưng lưu dữ liệu nhạy cảm qua dịch vụ KMS của bên khác).	– **Rủi ro không tuân thủ:** CSP không hỗ trợ có thể **không thông báo sự cố** cho khách hàng (khó tuân thủ NĐ 13 yêu cầu báo Bộ CA); hoặc **không chấp nhận yêu cầu kiểm tra an ninh** (khách hàng không có bằng chứng tuân thủ để trình cơ quan). – **Xung đột pháp lý:** Nếu CSP đặt trụ sở ở nước áp dụng luật xung đột (vd CLOUD Act của Mỹ), CSP có thể bị bắt buộc cung cấp dữ liệu khách hàng VN cho chính phủ họ mà **không được phép báo cho khách**. Điều này mâu thuẫn với yêu cầu bảo mật của VN và có thể gây tình huống khó xử (khách hàng vi phạm cam kết với người

Bước quyết định	Điều kiện/ Loại dữ liệu	Kết luận sử dụng	Thủ tục/Hồ sơ yêu cầu trước khi chuyển	Kiểm soát tối thiểu cần áp dụng	Rủi ro còn lại
	region đó nếu không được phép.				dùng VN nếu dữ liệu bị tiết lộ). – **Phụ thuộc nhà cung cấp:** CSP không cam kết tuân thủ có thể đơn phương thay đổi chính sách (vd ngừng dịch vụ ở VN do rủi ro pháp lý). Khách hàng phải chuẩn bị **kế hoạch thoát** để không bị gián đoạn nếu điều đó xảy ra.

Nội dung trên cho thấy: Việc dùng public cloud nước ngoài **không bị cấm hoàn toàn**, nhưng doanh nghiệp phải **đáp ứng nhiều yêu cầu pháp lý** (đặc biệt về dữ liệu cá nhân) và **tự đánh giá mức độ rủi ro**. Khi nghi ngờ, **ưu tiên an toàn pháp lý**: chọn cloud trong nước hoặc kiến trúc hybrid để vừa tận dụng được ưu điểm cloud, vừa giữ tuân thủ.

Phân định một số khái niệm kỹ thuật trong bối cảnh pháp lý

Để áp dụng đúng luật, cần hiểu rõ các khái niệm kỹ thuật và cách luật điều chỉnh:

- **Storage vs. Processing vs. Remote Access:** Luật bảo vệ dữ liệu cá nhân định nghĩa **"Chuyển dữ liệu ra nước ngoài"** là hành vi **đưa dữ liệu cá nhân VN tới một địa điểm nằm ngoài lãnh thổ VN hoặc sử dụng một địa điểm ngoài lãnh thổ để xử lý dữ liệu** [69] . Như vậy, nếu chỉ **truy cập từ xa** vào dữ liệu lưu ở VN (VD: chuyên gia ở Mỹ truy cập vào server đặt tại VN) thì *chưa được coi là chuyển dữ liệu ra nước ngoài*, vì dữ liệu vẫn nằm trong lãnh thổ VN. Tuy nhiên, remote access vẫn tiềm ẩn nguy cơ lộ dữ liệu (qua màn hình, tải tệp tạm...) nên tổ chức phải kiểm soát (VPN an toàn, không lưu file cục bộ...). Còn **lưu trữ (storage)** hay **xử lý (processing)** trực tiếp trên hạ tầng ngoài lãnh thổ đều bị coi là "chuyển dữ liệu" và phải tuân thủ quy định chuyển dữ liệu (DPIA, thông báo...).

- **Cloud region tại VN vs. region ngoài VN:** Nếu CSP (như AWS, Azure) mở region ngay tại VN, dữ liệu lưu trong region đó **không bị coi là chuyển ra nước ngoài** và không phải làm thủ tục DPIA. Tuy nhiên, cần lưu ý: CSP nước ngoài có region VN vẫn chịu sự quản lý của công ty mẹ ở nước ngoài, nên

rủi ro về yêu cầu cung cấp dữ liệu theo luật nước ngoài vẫn có (dù dữ liệu vật lý ở VN). Ưu điểm của region VN là **độ trễ thấp, không lo đứt cáp**, và **cơ quan VN dễ yêu cầu cung cấp dữ liệu** (vì server ở VN có thể bị cưỡng chế theo luật VN). Doanh nghiệp nên xem region VN như một lựa chọn tốt cho dữ liệu đòi hỏi độ phản hồi nhanh và tuân thủ lưu trữ nội địa.

- **Encryption và quản lý khóa (BYOK/HYOK):** Mã hóa dữ liệu trước khi đưa lên cloud là biện pháp **giảm thiểu rủi ro đáng kể**. Tuy nhiên, về mặt **nghĩa vụ pháp lý**, mã hóa **không thay thế được yêu cầu thủ tục**. Ví dụ: Dữ liệu cá nhân dù mã hóa vẫn là dữ liệu cá nhân, đưa ra nước ngoài vẫn phải làm DPIA theo NĐ 13 (luật không có ngoại lệ "nếu mã hóa thì không tính chuyển dữ liệu"). Tuy vậy, nếu mã hóa với khóa do khách hàng giữ (HYOK), CSP và bên thứ ba không đọc được dữ liệu, điều này **giảm nguy cơ vi phạm** (dữ liệu khó bị lộ ở dạng rõ). Nhưng doanh nghiệp cần lưu ý: nếu cơ quan VN yêu cầu cung cấp dữ liệu dạng rõ phục vụ điều tra, doanh nghiệp phải giải mã được. Do đó BYOK/HYOK nên được triển khai sao cho doanh nghiệp (chứ không phải CSP) nắm khóa giải mã, sẵn sàng hợp tác với cơ quan chức năng khi cần.

- **Backup/Replication cross-border có được coi là "chuyển dữ liệu ra nước ngoài"?** Theo định nghĩa NĐ 13, **có**. Dù dữ liệu gốc vẫn ở VN, việc tạo một bản sao lưu trên máy chủ ở nước ngoài đồng nghĩa dữ liệu đó đã "được chuyển tới địa điểm ngoài lãnh thổ VN" [69] . Do đó, **sao lưu định kỳ sang cloud nước ngoài** cũng phải tuân thủ thủ tục như chuyển dữ liệu (cần DPIA, v.v.). Nhiều doanh nghiệp hiểu lầm rằng backup không phải chính thức "sử dụng" dữ liệu, nhưng luật không phân biệt – bất kỳ hình thức chuyển nào cũng tính. Nếu muốn tránh thủ tục phiền phức, doanh nghiệp có thể **mã hóa mạnh bản backup trước khi chuyển** và lưu giữ khóa riêng; tuy nhiên về pháp lý vẫn nên làm DPIA. Giải pháp khác: **backup ra cloud nội địa hoặc lưu trữ vật lý tại VN** để không vướng quy định chuyển dữ liệu.

Tóm lại, khi thiết kế giải pháp cloud, **cần tính đến các khía cạnh luật ngay từ đầu**: đặt region phù hợp, triển khai mã hóa, chuẩn bị quy trình DPIA nếu dùng hạ tầng nước ngoài, và **đào tạo nhận thức** cho đội kỹ thuật để không vô tình vi phạm (VD: không ai tự tiện chọn lưu log khách hàng ở server nước ngoài chỉ vì "tiện kỹ thuật").

C) Yêu cầu tuân thủ cho tổ chức sử dụng Public Cloud (Cloud Customer)

Dựa trên các quy định pháp luật đã phân tích, dưới đây là bảng tổng hợp các **"control requirements"** – yêu cầu kiểm soát mà tổ chức (khách hàng cloud) cần triển khai để tuân thủ. Các yêu cầu được chia làm 6 nhóm: (1) Quản lý phân loại & danh mục dữ liệu; (2) Quản lý chuyển dữ liệu qua biên giới; (3) Đánh giá và giám sát nhà cung cấp (CSP); (4) Yêu cầu an ninh cơ bản; (5) Vận hành quản trị tuân thủ; (6) Điều khoản hợp đồng & pháp lý.

Bảng: Yêu cầu kiểm soát tuân thủ Cloud

Nhóm/Yêu cầu	Nguồn luật tham chiếu	Mô tả biện pháp kiểm soát	Bằng chứng tuân thủ cần có	Trách nhiệm chính	Công cụ gợi ý
Data Classification & Inventory					
- **Xác định & phân loại dữ liệu** lưu trữ trên cloud	Luật ATTTM 2015; NĐ 85/2016; NĐ 13/2023 (Điều 2)	Xây dựng **danh mục dữ liệu** tổ chức dự kiến đưa lên cloud, phân loại theo các tiêu chí pháp lý: dữ liệu cá nhân (loại thường/ nhạy cảm theo NĐ 13) [13] ; dữ liệu mật nhà nước (nếu có); dữ liệu quan trọng nội bộ. Gán **mức độ nhạy cảm** hoặc **cấp độ hệ thống** (1-5) cho từng tập dữ liệu theo NĐ 85. Đánh dấu những dữ liệu **chịu ràng buộc lưu trữ nội địa** (nếu thuộc loại phải lưu tại VN).	*Tài liệu:* Danh sách các loại dữ liệu (Data Inventory) bao gồm trường thông tin, mức độ nhạy cảm, vị trí lưu trữ dự kiến. *Chính sách:* Văn bản phân loại dữ liệu (Data Classification Policy) quy định nhãn (Public/ Internal/ Confidential/ Restricted, hoặc tương đương cấp 1-5). *Quyết định phân loại BMNN:* nếu đơn vị có thông tin mật NN, cần văn bản xác định độ mật và phương án bảo vệ.	Chủ Data (Data Owner) tại các phòng ban cung cấp thông tin; Bộ phận An toàn thông tin/ Pháp chế tổng hợp. *Phê duyệt cuối:* Ban lãnh đạo phê duyệt bảng phân loại.	- Sử dụng **công cụ quản lý dữ liệu** (Data Mapping Tool, có thể là module trong giải pháp GRC) để lập và cập nhật inventory. - Các **template phân loại** dựa trên tiêu chuẩn ISO 27001/27701 (phù hợp với NĐ 13).

- **Đánh giá mức độ phù hợp lên cloud**	NĐ 85/2016; Luật BMNN; tiêu chuẩn ngành (NHNN, Bộ YT…)	Đối với từng nhóm dữ liệu/hệ thống trong inventory, đánh giá xem **đưa lên cloud công cộng có phù hợp không** dựa trên luật: + Dữ liệu nào **luật cấm đưa ra ngoài**: phải loại khỏi phạm vi cloud public (giữ on-prem hoặc cloud riêng). + Dữ liệu quan trọng cấp 4-5: cân nhắc cloud riêng/nội địa. + Dữ liệu DLCN: có thể đưa lên nhưng phải làm DPIA và kiểm soát chặt (như phần B). Đánh giá này cần được lập thành tài liệu (data placement decision) kèm lý do và biện pháp giảm thiểu	*Biên bản/ Report:* Báo cáo "Đánh giá rủi ro và khả năng đưa dữ liệu lên cloud" – liệt kê từng loại dữ liệu, quyết định: cho phép lên cloud hay không, nếu có thì lên **loại cloud nào** (public/ hybrid, nội địa/quốc tế), điều kiện kèm theo (mã hóa, được consent…). Ví dụ: "Dữ liệu khách hàng (PII) – cho phép trên AWS Singapore, điều kiện: hoàn thành DPIA, mã hóa mức trường nhạy cảm."	CIO/CTO dẫn dắt đánh giá kỹ thuật; CISO/ Pháp chế đánh giá rủi ro pháp lý; hội đồng CNTT phê duyệt quyết định.	- Sử dụng **ma trận ra quyết định** trên bảng tính, liệt kê dữ liệu vs tiêu chí (nhạy cảm, luật liên quan, rủi ro) để hỗ trợ thẩm định. - Công cụ **Data Discovery** (như Azure Information Protection, Vera) để quét nhận diện thông tin nhạy cảm trong tập dữ liệu, hỗ trợ phân loại.

Nhóm/Yêu cầu	Nguồn luật tham chiếu	Mô tả biện pháp kiểm soát	Bằng chứng tuân thủ cần có	Trách nhiệm chính	Công cụ gợi ý
		nếu vẫn chọn cloud.			

- **Quy định thời hạn lưu trữ & hủy dữ liệu**	Luật ANM 2018 (yêu cầu lưu log tối thiểu 12 tháng) [70] ; NĐ 13/2023 (quyền xóa dữ liệu)	Đặt ra **chính sách lưu trữ dữ liệu (data retention)** cho dữ liệu trên cloud, tuân thủ quy định: + Nhật ký truy cập hệ thống liên quan an ninh mạng lưu **tối thiểu 12 tháng** (theo NĐ 53/2022) [70] . + Dữ liệu cá nhân: chỉ lưu trong thời gian cần thiết cho mục đích, khi hết hạn hoặc rút consent phải xóa [67] . + Tuân thủ yêu cầu ngành: ví dụ dữ liệu kế toán lưu 10 năm (Luật Kế toán). Xây dựng lịch trình tự động **xóa/ hủy dữ liệu** trên cloud khi hết hạn, hoặc đưa về lưu trữ ngoại tuyến	*Chính sách Data Retention:* nêu rõ thời gian lưu cho từng loại dữ liệu; phương thức hủy an toàn (xóa không khôi phục, ghi đè). *Minh chứng:* Cấu hình trên cloud (ví dụ lifecycle policy của S3 bucket) cho thấy dữ liệu sẽ auto-delete sau X ngày. Log hoặc báo cáo xóa dữ liệu định kỳ hàng quý. *Biên bản hủy*: nếu hủy thủ công, có biên bản xác nhận.	Bộ phận **Quản trị dữ liệu (Data Governance)** hoặc CNTT chịu trách nhiệm thực thi retention policy. Chủ dữ liệu phê duyệt trước khi hủy.	- Tận dụng **tính năng lifecycle** của dịch vụ cloud (S3 Lifecycle rules, Azure Blob retention, etc.) để tự động lưu trữ lạnh/xóa. - Công cụ **SIEM** theo dõi log lưu trữ, cảnh báo nếu log sắp quá hạn. - **Data retention schedule** (file Excel/ SharePoint) để theo dõi thủ công kết hợp.

Nhóm/Yêu cầu	Nguồn luật tham chiếu	Mô tả biện pháp kiểm soát	Bằng chứng tuân thủ cần có	Trách nhiệm chính	Công cụ gợi ý
		an toàn nếu cần lưu lâu.			
Cross-Border Data Transfer Management					

- **Đánh giá tác động & đăng ký chuyển dữ liệu**	NĐ 13/2023, Điều 25 [29] [30] ; Quy định ngành (TT NHNN 09/2020 yêu cầu báo cáo NHNN trước khi dùng cloud) [64]	Khi có nhu cầu lưu hoặc xử lý dữ liệu tại region nước ngoài, thực hiện quy trình: 1) **Data Transfer Impact Assessment (DTIA)**: Phân tích các mục tiêu, rủi ro như yêu cầu Điều 25 NĐ 13. Lập hồ sơ theo mẫu (Mẫu 06). 2) **Nộp hồ sơ cho Bộ Công an (A05)**: Gửi bản chính DPIA trong vòng 60 ngày từ khi bắt đầu chuyển [30] . 3) **Thông báo sau chuyển**: Gửi văn bản thông báo thông tin liên hệ và tình trạng chuyển xong [33] . Nếu Bộ CA yêu cầu bổ sung, hoàn thiện trong 10 ngày [34] . Riêng ngành NH:	*Hồ sơ DPIA:* tài liệu dày đủ các mục a) đến h) Điều 25(2) NĐ 13 [31] [32] , có chữ ký người chịu trách nhiệm. *Xác nhận gửi:* biên nhận gửi hồ sơ qua bưu điện hoặc Cổng TTĐT Bộ CA (khi có). *Thông báo hoàn tất:* bản sao văn bản đã gửi thông báo sau khi chuyển (có dấu gửi). *Báo cáo NHNN:* (đối với ngân hàng) bản sao báo cáo rủi ro đã nộp NHNN và biên nhận.	Bộ phận **Pháp chế** phối hợp **CNTT** lập hồ sơ DPIA. Chỉ định **Data Protection Officer (DPO)** hoặc người phụ trách bảo vệ DL (theo NĐ 13 yêu cầu đối với DN lớn) chịu trách nhiệm gửi và làm việc với cơ quan NN. Ngành NH: Giám đốc CNTT phê duyệt báo cáo gửi NHNN.	- Sử dụng **mẫu DPIA** (theo phụ lục NĐ 13 hoặc tham khảo GDPR DPIA template) điền sẵn các nội dung. - Công cụ **GRC** có module Privacy (như OneTrust, TrustArc) có thể hỗ trợ quy trình DPIA, quản lý việc phê duyệt và lưu trữ hồ sơ. - Hệ thống **quản lý văn bản** của doanh nghiệp để gửi công văn Bộ CA, lưu số hiệu công văn.

Nhóm/Yêu cầu	Nguồn luật tham chiếu	Mô tả biện pháp kiểm soát	Bằng chứng tuân thủ cần có	Trách nhiệm chính	Công cụ gợi ý
		Trước khi dùng cloud (kể cả nội địa hay ngoại), TCTD phải gửi **báo cáo đánh giá rủi ro lên NHNN** (Cục CNTT) [64].			

- **Kiểm soát chuyển dữ liệu trong vận hành**	NĐ 13/2023 (Điều 25.7, 25.8) [35] [36]; Luật ATTTM	Sau khi được phép chuyển, tổ chức thiết lập kiểm soát thường xuyên: – **Danh mục dữ liệu/ứng dụng chuyển xuyên biên giới**: duy trì danh sách các ứng dụng, flow dữ liệu nào đang đẩy ra nước ngoài. Bất kỳ thay đổi (thêm loại dữ liệu, đổi nhà cung cấp) phải **cập nhật DPIA và thông báo Bộ CA** trong vòng 10 ngày [71]. – **Giám sát lưu lượng**: cấu hình hệ thống DLP (Data Loss Prevention) hoặc firewall để phát hiện nếu có dữ liệu nhạy cảm bị chuyển ra ngoài không qua kênh đã phê duyệt. – **Kiểm**	*Báo cáo đánh giá định kỳ:* mỗi năm lập báo cáo nội bộ về tình trạng tuân thủ chuyển dữ liệu: đã chuyển những gì, có sự cố nào không, có đáp ứng đúng cam kết DPIA không. *Log giám sát:* Nhật ký của DLP hoặc firewall cho thấy lưu lượng ra nước ngoài được kiểm soát. Bất thường (nếu có) kèm phân tích xử lý. *Biên bản đào tạo:* đào tạo nhân viên về quy trình chuyển dữ liệu ra nước ngoài, nhằm tránh trường hợp họ vô tình dùng công cụ cloud ngoài luồng.	Bộ phận **An ninh thông tin** thiết lập giám sát kỹ thuật (DLP). **DPO/ Pháp chế** phối hợp làm báo cáo hàng năm và gửi Bộ CA nếu có yêu cầu. **Quản lý các bộ phận** đảm bảo nhân viên không dùng trái phép dịch vụ cloud ngoài quy trình.	- Triển khai **DLP software** (Symantec, Microsoft Purview DLP) giám sát email, upload web có chứa dữ liệu nhạy cảm ra ngoài. - Sử dụng **Cloud Access Security Broker (CASB)** để quản lý các cloud service được phép, chặn dịch vụ không kiểm soát (shadow IT). - Dùng **thiết bị firewall** có chức năng geo-IP filtering để chặn truy cập server nội bộ từ IP nước ngoài nếu không cần thiết.

Nhóm/Yêu cầu	Nguồn luật tham chiếu	Mô tả biện pháp kiểm soát	Bằng chứng tuân thủ cần có	Trách nhiệm chính	Công cụ gợi ý
		tra hằng năm: đánh giá 1 lần/ năm việc chuyển dữ liệu có đúng như hồ sơ đã nộp không (Bộ CA cũng có thể kiểm tra định kỳ) [35]. Nếu phát hiện vi phạm (chuyển nhiều hơn phạm vi cho phép, bị lộ dữ liệu…), phải **tự nguyện tạm dừng chuyển** và báo cáo cơ quan chức năng.			
Vendor/CSP Due Diligence					

- **Tiêu chí lựa chọn CSP**	NĐ 13/2023 (Điều 39) – yêu cầu bên xử lý có biện pháp bảo vệ [26] ; TT 09/2020 NHNN – CSP phải có chứng chỉ ATTT, hạ tầng đáp ứng luật [62] ; Luật VT 2023 – CSP cloud phải đăng ký dịch vụ VT, tuân thủ ATTT, bảo vệ DL cá nhân [72]	Trước khi ký hợp đồng với CSP, tổ chức tiến hành **đánh giá nhà cung cấp** tập trung vào: – **Tuân thủ pháp luật VN:** CSP đã có **pháp nhân hoặc đăng ký thuế** tại VN chưa? (Luật Viễn thông 2023 yêu cầu dịch vụ cloud phải đăng ký tại Bộ TT&TT) [73] . CSP có chính sách tuân thủ NĐ 13 không (nhiều CSP quốc tế phát hành addendum GDPR nhưng chưa chắc tương thích NĐ13). – **Chứng chỉ bảo mật:** Kiểm tra CSP có các chứng nhận quốc tế quan trọng: **ISO 27001** (hệ thống ISMS chung), **ISO**	*Báo cáo đánh giá NCC:* Một bảng điểm (scorecard) cho các tiêu chí: Pháp lý (đk kinh doanh tại VN, tuân thủ VT, thuế), Bảo mật (danh sách chứng chỉ, tiêu chuẩn đáp ứng), Kỹ thuật (DC location, SLA uptime, hỗ trợ), Tuân thủ dữ liệu (hỗ trợ DPA, tiêu chuẩn quốc tế). Báo cáo nêu rõ điểm mạnh/ yếu và **quyết nghị chọn** hay không. *Bằng chứng từ NCC:* bản sao chứng chỉ ISO, báo cáo kiểm toán bên thứ ba (CSP có thể cung cấp "SOC 2 Type II report" dưới NDA), tài liệu kiến trúc bảo mật CSP. *Biên bản PoC:* nếu có thử nghiệm	**Nhóm đánh giá NCC**: gồm IT, An toàn TT, Pháp chế, Vận hành cùng đánh giá. Quyết định cuối bởi **Ban lãnh đạo** (CIO/ CTO) ký chọn nhà CC dựa trên khuyến nghị.	- Sử dụng **bảng câu hỏi đánh giá bảo mật nhà cung cấp** (Vendor Security Assessment Questionnaire) – có thể dùng mẫu theo tiêu chuẩn như CAIQ (Consensus Assessments Initiative Questionnaire) của CSA – gửi cho CSP điền. - Công cụ **Third-party risk management** (các nền tảng như OneTrust, BitSight) để theo dõi liên tục chỉ số an toàn của CSP (ví dụ điểm an ninh mạng công khai). - Tham khảo **danh sách xếp hạng**: Gartner Magic Quadrant, CSA STAR Registry (nếu CSP có tham gia) để biết mức độ uy tín.

		27017 (kiểm soát an ninh cho cloud), **ISO 27018** (bảo vệ thông tin cá nhân trên cloud); **SOC 2** báo cáo loại 2; **PCI-DSS** (nếu lưu dữ liệu thẻ thanh toán)... Các chứng chỉ còn hiệu lực, do tổ chức độc lập cấp. – **Vị trí trung tâm dữ liệu & hạ tầng:** Xác định CSP cung cấp dịch vụ từ DC nào (trong nước hay nước ngoài, Tier mấy, có dự phòng ra sao). Nếu phục vụ CQNN, ưu tiên CSP có DC tại VN, đạt chuẩn **Tier III hoặc cao hơn**. – **Năng lực kỹ thuật và hỗ trợ:** CSP có khả năng tách biệt dữ liệu khách hàng (multi-	dịch vụ trước, kèm kết quả.

Nhóm/Yêu cầu	Nguồn luật tham chiếu	Mô tả biện pháp kiểm soát	Bằng chứng tuân thủ cần có	Trách nhiệm chính	Công cụ gợi ý
		tenancy isolation) [63], mã hóa, và log audit cung cấp cho khách? Có hỗ trợ 24/7 và kênh liên lạc sự cố? – **Uy tín tuân thủ:** Tra cứu xem CSP từng vi phạm bảo mật nào chưa, có bị kiện về xâm phạm dữ liệu không.			

- **Quản lý rủi ro bên thứ ba liên tục**	NĐ 13/2023 (Điều 42) – tổ chức phải phối hợp xử lý vi phạm DL [41] ; TT 09/2020 NHNN – yêu cầu đánh giá tuân thủ hàng năm [74] ; ISO 27001 A.15	Sau khi thuê dịch vụ cloud, cần **giám sát và làm việc thường xuyên với CSP**: – **Điều khoản báo cáo định kỳ:** Yêu cầu CSP cung cấp báo cáo **trạng thái tuân thủ** hàng năm: ví dụ chứng chỉ ISO còn hiệu lực, kết quả kiểm toán bảo mật mới nhất, báo cáo kiểm tra xâm nhập (nếu có)... – **Quy trình sự cố:** Thiết lập kênh thông báo sự cố. Nếu CSP có sự cố (data breach, outage kéo dài) ảnh hưởng khách hàng, cần ngay lập tức nhận thông tin. Yêu cầu trong hợp đồng mốc thời gian (VD: thông	*Báo cáo tuân thủ NCC hàng năm:* tổng hợp các tài liệu CSP cung cấp, đánh giá mức độ đáp ứng cam kết. *Biên bản họp đánh giá NCC:* cuộc họp (ít nhất hàng năm) với đại diện CSP để rà soát hiệu quả dịch vụ, sự cố đã xảy ra, các vấn đề tuân thủ. *Kế hoạch thoát:* tài liệu nội bộ mô tả các bước sao lưu dữ liệu, chuyển sang hệ thống khác, thời gian dự kiến, ai phụ trách. *Log sự cố:* nếu có sự cố, lưu trữ thông báo của CSP, phân tích nguyên nhân và biện pháp CSP khắc phục.	Bộ phận **Quản trị rủi ro bên thứ ba** (thuộc Risk/ Compliance) giữ liên lạc chính với CSP về vấn đề tuân thủ. **IT Operation** lo theo dõi chất lượng dịch vụ (SLA, downtime). **Ban lãnh đạo** (CIO) định kỳ gặp phía CSP (QBR – quarterly business review).	- Sử dụng **công cụ quản lý nhà cung cấp** (Vendor Management in ServiceNow, Archer, hoặc đơn giản Excel tracker) để theo dõi thời hạn chứng chỉ CSP, nhắc nhở khi sắp hết hạn. - Thiết lập **SLM (Service Level Monitoring)**: dùng công cụ CloudWatch, Azure Monitor... giám sát uptime, hiệu năng, so với SLA cam kết, tạo báo cáo tự động. - Bảng checklist **Exit Plan** để luyện tập giả định (ví dụ diễn tập khôi phục dữ liệu từ backup ngoài, đo thời gian và độ đầy đủ).

		báo trong 24h từ khi phát hiện sự cố bảo mật). – **Đánh giá tuân thủ định kỳ:** Thực hiện **đánh giá bên thứ ba hàng năm** – có thể là yêu cầu tự đánh giá (CSP điền bảng) hoặc thực hiện audit độc lập. Đối với NH: bắt buộc đánh giá tuân thủ thỏa thuận mỗi năm, có thể dựa trên kết quả audit CNTT độc lập của CSP [74]. – **Quản lý thay đổi NCC:** Nếu CSP thay đổi dịch vụ (thêm sub-processor ở nước khác, thay đổi chính sách bảo mật), phải có quy trình tiếp nhận thông tin và đánh giá lại rủi ro, cập nhật hợp đồng/ DPIA nếu

Nhóm/Yêu cầu	Nguồn luật tham chiếu	Mô tả biện pháp kiểm soát	Bằng chứng tuân thủ cần có	Trách nhiệm chính	Công cụ gợi ý
		cần. – **Kế hoạch thoát (Exit Plan):** Luôn có sẵn phương án chuyển đổi hoặc rút dữ liệu khỏi CSP một cách an toàn nếu rủi ro vượt ngưỡng (VD CSP bị mua lại bởi công ty không đáng tin, hoặc yêu cầu pháp lý mới làm dịch vụ không còn phù hợp).			
Security Baseline (Cloud Security)					

- **Kiểm soát truy cập & Danh tính (IAM)**	Luật ATTTM 2015 (yêu cầu bảo đảm an toàn truy cập); NĐ 13 (nguyên tắc chỉ cho phép người có thẩm quyền xử lý DL) [38]	Thiết lập chính sách **Quản lý tài khoản và truy cập** chặt chẽ trên môi trường cloud: – **Nguyên tắc tối thiểu (Least Privilege):** Mỗi người dùng/cloud service account chỉ được cấp quyền tối thiểu cần thiết. Không dùng tài khoản root hay quyền admin tổng quát cho tác vụ hàng ngày. – **Quản lý tập trung danh tính:** Tích hợp cloud IAM với hệ thống Single Sign-On nội bộ để kiểm soát tập trung (VD: dùng Azure AD/Google Workspace làm SSO). – **Xác thực đa yếu tố (MFA):** Bắt buộc MFA cho mọi	*Chính sách IAM:* văn bản quy định việc tạo tài khoản, phê duyệt cấp quyền, sử dụng MFA, quản lý mật khẩu/khóa. *Cấu hình hệ thống:* Bằng chứng ảnh chụp màn hình hoặc báo cáo từ cloud console cho thấy: MFA = Enabled cho user quan trọng, không có user chung, quyền admin chỉ thuộc về nhóm hẹp. *Báo cáo soát xét quyền:* file excel hoặc tool output liệt kê user và quyền, có nhận xét của reviewer, thay đổi đã thực hiện. *Biên bản huấn luyện người dùng:* về bảo mật mật khẩu, sử dụng SSO.	**Quản trị viên Cloud (Cloud Admin)** thực hiện cấu hình IAM theo chính sách. **Bộ phận IT Helpdesk** phối hợp quản lý vòng đời tài khoản. **Bộ phận Kiểm soát nội bộ/ATTT** định kỳ kiểm tra.	- Sử dụng **công cụ IAM** tích hợp: AWS IAM, Azure AD Privileged Identity Management (PIM) để cấp quyền tạm thời khi cần. - **Password manager/Vault**: HashiCorp Vault, AWS Secrets Manager để lưu secret. - **Cloud security posture management (CSPM)**: ví dụ Prisma Cloud, AWS Security Hub – kiểm tra thiết lập IAM tuân thủ best practice.

Nhóm/Yêu cầu	Nguồn luật tham chiếu	Mô tả biện pháp kiểm soát	Bằng chứng tuân thủ cần có	Trách nhiệm chính	Công cụ gợi ý
		tài khoản quản trị cloud và tài khoản người dùng truy cập dữ liệu quan trọng. – **Quản lý khóa API/ secret:** Lưu trữ khóa API, mật khẩu dịch vụ trong **vault an toàn**; thường xuyên xoay vòng. Không hard-code secret trong code. – **Theo dõi và thu hồi quyền:** Định kỳ (hàng quý) soát lại quyền user trên cloud, thu hồi tài khoản không dùng, giảm quyền các tài khoản dư thừa.			

- **Mã hóa dữ liệu & Quản lý khóa**	NĐ 13 (biện pháp kỹ thuật bảo vệ DL) [75] ; yêu cầu ngành tài chính (PCI-DSS)	Áp dụng mã hóa cho dữ liệu **ở trạng thái lưu trữ (at rest)** và **khi truyền (in transit)**: – **Mã hóa khi lưu trữ:** Bật tính năng mã hóa của cloud cho mọi ổ đĩa, CSDL, bucket. Sử dụng **các thuật toán mạnh** (AES-256). – **Tùy chọn BYOK/ HSM:** Nếu dữ liệu rất nhạy cảm, sử dụng khóa mã hóa do doanh nghiệp quản lý (Bring Your Own Key) hoặc thiết bị HSM đặt tại VN để quản lý khóa (HYOK – Hold Your Own Key), nhằm ngăn CSP tiếp cận khóa. – **Mã hóa khi truyền:** Mọi kết nối từ người dùng tới ứng	*Sơ đồ kiến trúc bảo mật:* mô tả điểm nào dữ liệu được mã hóa, loại mã hóa, ai giữ khóa. *Thiết lập trong cloud:* ảnh chụp hoặc output lệnh CLI chứng minh các volume, database đã được mã hóa (vd "Encryption: ENABLED"). *Báo cáo kiểm thử truyền thông:* chạy công cụ (Qualys SSL Labs hoặc Nmap) để kiểm tra chỉ chấp nhận TLS >=1.2, không có ciphers yếu. *Quy trình quản lý khóa:* tài liệu về cách tạo, lưu, xoay, hủy khóa; log lưu trữ cho thấy lần xoay khóa gần nhất, người phê duyệt. *Báo cáo kiểm toán nội bộ:* nếu có	**Kiến trúc sư bảo mật Cloud** thiết kế việc mã hóa và quản lý khóa. **Quản trị viên Cloud** thực hiện thiết lập mã hóa trên dịch vụ. **Bộ phận ATTT** (hoặc đội Crypto) quản trị các HSM, kho khóa tập trung.	- Sử dụng dịch vụ **KMS (Key Management Service)** do cloud cung cấp (AWS KMS, Azure Key Vault) kết hợp BYOK: upload key do mình tạo. - Triển khai **Hardware Security Module (HSM)** chuyên dụng (AWS CloudHSM, hoặc HSM on-prem kết nối cloud) cho các khóa root quan trọng. - **DLP & Tokenization tools**: nếu cần ẩn danh thay vì mã hóa (để vẫn phân tích được dữ liệu), có thể dùng tokenization với kho giữ map trên-prem.

		dụng cloud hoặc giữa các dịch vụ đều phải dùng giao thức bảo mật (HTTPS/ TLS 1.2 trở lên, SSH...). Cấm giao thức không mã hóa. – **Quản lý vòng đời khóa:** Đặt chính sách đổi khóa định kỳ (ví dụ 1-2 năm), hủy khóa an toàn khi không dùng. Khóa phải được backup bảo mật. – **Mã hóa cấp ứng dụng (nếu cần):** Đối với thông tin cá nhân nhạy cảm (như số CMND, dữ liệu sức khỏe), ngoài mã hóa ổ đĩa có thể **mã hóa ở mức trường dữ liệu** trong CSDL (field-level encryption) để dữ liệu đó luôn ở	đánh giá độc lập, xác nhận tuân thủ chính sách mã hóa.

Nhóm/Yêu cầu	Nguồn luật tham chiếu	Mô tả biện pháp kiểm soát	Bằng chứng tuân thủ cần có	Trách nhiệm chính	Công cụ gợi ý
		dạng mã hóa ngay cả khi truy cập bằng công cụ quản trị cloud.			

- **Logging, Giám sát an toàn & Ứng phó sự cố**	Luật ANM 2018 (lưu log hệ thống tối thiểu 12 tháng) [3]; NĐ 13 (thông báo vi phạm ngay) [76]	Thiết lập khả năng **giám sát liên tục** hoạt động trên cloud và **quản lý sự cố**: – **Kích hoạt đầy đủ log**: Bật log cho mọi dịch vụ cloud (VD: AWS CloudTrail, VPC Flow Logs, CloudWatch; Azure Monitor, Activity Logs…). Đảm bảo log ghi nhận được **hoạt động quan trọng**: đăng nhập, tạo/sửa/xóa tài nguyên, truy cập dữ liệu quan trọng, thay đổi quyền. – **Lưu trữ tập trung log**: Đẩy log về hệ thống SIEM tập trung tại VN để phân tích (vừa đáp ứng lưu trữ nội địa theo Luật ANM, vừa tiện điều tra).	*Thiết lập log:* Ảnh chụp bảng cấu hình cho thấy CloudTrail "All regions, All events = On", lưu vào S3; Azure Activity Log streaming về Log Analytics. *Log mẫu:* file log minh họa sự kiện (vd JSON log ghi lại hành động xóa VM với thông tin user, timestamp). *Báo cáo giám sát hằng ngày:* từ SIEM (vd số sự kiện cảnh báo, không có bất thường hoặc có và đã xử lý). *Kế hoạch ứng cứu sự cố:* văn bản hoặc sơ đồ các bước (thông báo ai, thực hiện thao tác gì), có phân công vai trò (RACI). *Báo cáo*	**Đội Vận hành An ninh (SOC)** chịu trách nhiệm triển khai logging, giám sát. **DevOps/ CloudOps** phối hợp cấu hình dịch vụ log và phản ứng kỹ thuật khi có cảnh báo (tắt máy, chặn IP…). **Ban chỉ đạo ứng cứu sự cố** (CIO/CISO đứng đầu) ra quyết định lớn (thông báo khách hàng, cơ quan).	- Sử dụng **dịch vụ giám sát tích hợp**: AWS GuardDuty, Azure Security Center – để phát hiện bất thường tự động bằng ML. - Triển khai hệ thống **SIEM** tại VN (ví dụ Splunk, Elastic Stack, ArcSight) nhận log từ cloud qua cổng bảo mật. - Dùng **SOAR** (Security Orchestration, Automation and Response) để tự động hóa phản ứng ban đầu (ví dụ phát hiện rò rỉ key tự động khoá tài khoản). - Công cụ **Incident Response Platform** (TheHive, Cortex) để quản lý quy trình IR và bằng chứng.

		Lưu log >= 12 tháng [70] . – **Giám sát sự kiện bất thường:** Định nghĩa use-case cảnh báo: ví dụ đăng nhập thất bại nhiều, tạo máy chủ mới ngoài giờ, tải lượng lớn dữ liệu từ storage. SIEM hoặc dịch vụ cảnh báo cloud (CloudWatch Alarms) gửi thông báo cho đội ứng trực. – **Quy trình phản ứng sự cố:** Xây dựng playbook cho các tình huống sự cố cloud: xâm nhập tài khoản, mã độc mã hóa dữ liệu, lộ dữ liệu... Bao gồm các bước cô lập, thu thập bằng chứng, thông báo lãnh đạo và cơ quan NN nếu có dữ	*diễn tập:* tài liệu mô tả kịch bản, kết quả diễn tập xử lý sự cố cloud (ít nhất 1 lần/ năm).

Nhóm/Yêu cầu	Nguồn luật tham chiếu	Mô tả biện pháp kiểm soát	Bằng chứng tuân thủ cần có	Trách nhiệm chính	Công cụ gợi ý
		liệu cá nhân bị lộ (thông báo Bộ CA kịp thời) [76]. – **Diễn tập định kỳ:** Thực hiện drill giả lập sự cố (ví dụ khóa tài khoản admin bị lộ, hoặc xóa nhầm dữ liệu) để kiểm tra khả năng phản ứng và cải thiện.			

- **Quản lý cấu hình, điểm yếu và sao lưu**	Luật ATTTM (yêu cầu quản lý cấu hình, phòng chống mã độc, sao lưu dự phòng); NĐ 85/2016 (dự phòng, khôi phục sau thảm họa) [52]	Thiết lập **cấu hình an toàn chuẩn** cho môi trường cloud và duy trì liên tục: – **Baseline cấu hình bảo mật:** Áp dụng hardening cho OS trên máy ảo (theo CIS Benchmark), database (tắt dịch vụ không cần, dùng mật khẩu mạnh…). Sử dụng mẫu "secure image" cho VM. – **Quản lý bản vá:** Theo dõi và cập nhật bản vá hệ điều hành, ứng dụng trên cloud định kỳ (ví dụ hàng tháng), đặc biệt vá ngay các lỗ hổng nghiêm trọng (CVE nguy cơ cao). Nếu dùng dịch vụ PaaS không tự vá được, theo	*Danh sách tài sản & cấu hình chuẩn:* có bảng liệt kê các loại máy chủ, db… và đường dẫn đến baseline config/ hardening guide áp dụng cho từng loại. *Báo cáo quét lỗ hổng:* file PDF kết quả quét hàng quý, thể hiện không còn lỗ hổng mức cao (hoặc có và đã xử lý ghi chú). *Bằng chứng vá:* log từ hệ thống quản lý bản vá (WSUS, etc.) hoặc ảnh chụp version phần mềm trước/ sa u khi cập nhật. *Kế hoạch backup:* sơ đồ luồng backup (nguồn nào, lưu trữ ở đâu, tần suất); log backup (thành công hay lỗi); báo	**DevOps/Cloud Infrastructure Team** chịu trách nhiệm cấu hình hệ thống an toàn, vá và backup. **Security Team** giám sát, kiểm tra độc lập (qua quét lỗ hổng, pentest thuê ngoài). **Ban lãnh đạo CNTT** phê duyệt chính sách backup/DR và cung cấp nguồn lực.	- Sử dụng **Infrastructure as Code (IaC)**: viết mã (Terraform, CloudFormation) triển khai môi trường cloud với cấu hình bảo mật tích hợp, tránh cấu hình tay sai lệch. - **Config Management Tools**: Ansible, Chef – áp dụng các playbook hardening tự động cho server. - **Vulnerability Management System**: triển khai nền tảng (QualysGuard, Nessus Manager) để lịch quét tự động và theo dõi khắc phục. - **Backup Service**: dùng dịch vụ backup của cloud (AWS Backup, Azure Backup) kết hợp lưu offline; hoặc dùng giải pháp bên ngoài (Veeam) quản lý tập trung.

		dõi thông báo từ CSP. – **Quét và kiểm tra điểm yếu:** Chạy **bộ quét lỗ hổng** (Qualys, Nessus) định kỳ trên IP/ host cloud quan trọng. Kết hợp pentest bên thứ ba 1-2 lần/năm cho ứng dụng nhạy cảm. – **Chống mã độc & bảo vệ endpoint cloud:** Cài đặt agent anti-malware trên các VM, bật tính năng anti-virus cho storage (nếu có). Thiết lập EDR (Endpoint Detection & Response) trên server quan trọng để phát hiện hành vi bất thường. – **Sao lưu & khôi phục:** Triển khai quy trình backup	cáo thử khôi phục thành công. *Biên bản kiểm thử DR:* nếu có bài test DR chuyển sang môi trường backup (bao nhiêu thời gian, kết quả đạt được).

Nhóm/Yêu cầu	Nguồn luật tham chiếu	Mô tả biện pháp kiểm soát	Bằng chứng tuân thủ cần có	Trách nhiệm chính	Công cụ gợi ý
		định kỳ dữ liệu và cấu hình: ít nhất **theo nguyên tắc 3-2-1** (3 bản, 2 loại lưu trữ, 1 ở offsite). Lưu một bản backup trên vùng khác (có thể là cloud khác hoặc DC nội bộ). Mã hóa backup và **diễn tập khôi phục** định kỳ (đảm bảo backup thực sự dùng được khi cần).			
Governance & Compliance Operations					

- **Cơ cấu tổ chức & trách nhiệm (RACI) rõ ràng**	NĐ 13 (DN > vừa phải chỉ định nhân sự/bộ phận bảo vệ DL); ISO 27001 A.5	Thiết lập **bộ máy quản trị tuân thủ cloud**: – **Chỉ định Data Protection Officer/ Team:** Với tổ chức lớn, cần một cán bộ hoặc nhóm chuyên trách bảo vệ dữ liệu cá nhân (theo NĐ 13 khuyến nghị với DN vừa và nhỏ cũng hướng tới, DN lớn gần như bắt buộc). Người này chịu trách nhiệm theo dõi tuân thủ NĐ 13, làm đầu mối với cơ quan NN. – **Phân định vai trò an toàn cloud:** Rõ người/đội phụ trách *quản trị hạ tầng cloud*, *an ninh thông tin*, *pháp chế*, *quản lý rủi ro*, *IT audit*. Xác định RACI cho các	*Quyết định bổ nhiệm:* văn bản bổ nhiệm **Cán bộ bảo vệ dữ liệu cá nhân** (nêu rõ tên, chức vụ, nhiệm vụ) nếu có. *Sơ đồ tổ chức:* organogram đánh dấu các vai trò liên quan cloud compliance, đường dây báo cáo (ví dụ DPO báo cáo ban GĐ). *Ma trận RACI:* bảng liệt kê các hoạt động (DPIA, đánh giá NCC, xử lý yêu cầu dữ liệu…) với cột R, A, C, I tương ứng phòng ban/ cá nhân. *Biên bản họp ban chỉ đạo:* nếu có ban, lưu biên bản cuộc họp định kỳ/ quyết nghị quan trọng về cloud.	**Ban Giám đốc** phê duyệt cơ cấu và bổ nhiệm nhân sự chính (DPO, nhóm ATTT). **DPO/ Trưởng ATTT** xây dựng ma trận RACI và phổ biến trong nội bộ. **Các trưởng bộ phận liên quan** (CNTT, Pháp chế, Nhân sự…) phối hợp phân công người trong nhóm mình.	- Sử dụng **RACI matrix template** (Excel hoặc bảng trong policy) liệt kê rõ. - Công cụ quản lý sơ đồ tổ chức (**Org chart tool** như Visio hoặc phần mềm HR) để cập nhật khi nhân sự thay đổi. - Dùng **phần mềm quản trị công việc** (Jira, Trello) để gán nhiệm vụ cụ thể cho từng người trong các quy trình (ví dụ ticket thực hiện DPIA).

	quy trình: ví dụ DPIA – Responsible: Pháp chế, Accountable: DPO, Consulted: IT, Informed: Ban GĐ. – **Ban chỉ đạo chuyển đổi cloud:** Nếu dự án lớn, lập ban chỉ đạo bao gồm lãnh đạo CNTT, đại diện pháp chế, đại diện kinh doanh. Ban này duyệt các quyết định lớn (chọn CSP, chấp thuận đưa dữ liệu loại A lên cloud, xử lý sự cố lớn). – **Liên hệ cơ quan quản lý:** Chỉ định người phụ trách làm đầu mối với Bộ TT&TT, Bộ CA về an toàn mạng, dữ liệu (theo luật An ninh mạng có thể cử đầu mối hợp tác).	

- **Chương trình đào tạo & nhận thức**	NĐ 13 (yêu cầu nâng cao nhận thức bảo vệ DL) [77] ; tiêu chuẩn ISO 27001 A.7	Triển khai **đào tạo định kỳ** cho nhân viên về các chính sách và kỹ năng tuân thủ cloud: – **Đào tạo cho quản trị viên kỹ thuật:** nội dung về cấu hình an toàn cloud, cập nhật các quy định mới (ví dụ hướng dẫn Điện toán đám mây của Bộ TT&TT), các case study sự cố. – **Đào tạo cho nhân viên xử lý dữ liệu:** nhấn mạnh trách nhiệm bảo mật DLKH trên cloud, quy định về chuyển dữ liệu (nhân viên không tự ý dùng Google Drive cá nhân, v.v.), quy trình báo cáo sự cố. – **Diễn tập ứng cứu**: ngoài đào	*Kế hoạch đào tạo hàng năm:* tài liệu liệt kê các chủ đề, đối tượng, thời lượng đào tạo về cloud compliance. *Tài liệu đào tạo:* slide, video, cẩm nang... đã dùng trong buổi training. *Danh sách tham dự:* bảng ký tên hoặc report từ LMS cho thấy ai đã hoàn thành khóa học. *Kết quả quiz:* thống kê điểm đánh giá nhận thức trước/sau đào tạo. *Bằng chứng truyền thông:* email bản tin nội bộ nhắc nhở về chính sách cloud, poster, infographic lan tỏa văn hóa an toàn.	**Bộ phận Nhân sự** phối hợp **Bộ phận ATTT/ Compliance** xây dựng chương trình đào tạo. Giảng viên có thể từ **nhóm CNTT/ATTT nội bộ**, hoặc thuê chuyên gia ngoài (nhất là cho quản trị viên cần kỹ năng mới). **Quản lý các phòng ban** đảm bảo nhân viên tham gia đầy đủ.	- Sử dụng **Learning Management System (LMS)** (VD: Moodle, Microsoft Viva Learning) để triển khai các khóa e-learning về bảo mật cloud và theo dõi kết quả. - Nội dung có thể tham khảo từ các khóa quốc tế (Coursera, Cybrary) hoặc khuyến nghị của CSA. - Thường xuyên gửi **bản tin an toàn**: VD hàng tháng một tip (như "5 lưu ý khi dùng Google Drive để chia sẻ dữ liệu công ty"). - Tổ chức **Ngày hội ATTT**: mời chuyên gia trình bày về rủi ro cloud, kết hợp game/quiz tạo hứng thú.

		tạo lý thuyết, tổ chức diễn tập sự cố an toàn thông tin trên cloud (như đã nêu ở Security Baseline) với sự tham gia của các nhóm để mọi người biết vai trò. – **Kiểm tra kiến thức:** định kỳ kiểm tra nhanh (quizzes) về nhận thức an toàn thông tin cloud, pháp luật dữ liệu. Ai điểm kém bổ sung training. – **Cập nhật liên tục:** khi có luật mới (VD nếu VN ban hành Luật Bảo vệ dữ liệu cá nhân trong tương lai thay NĐ13) hoặc chính sách nội bộ mới, phải thông báo và nếu cần tổ chức lớp học cho	

Nhóm/Yêu cầu	Nguồn luật tham chiếu	Mô tả biện pháp kiểm soát	Bằng chứng tuân thủ cần có	Trách nhiệm chính	Công cụ gợi ý
		nhân viên liên quan.			

- **Giám sát tuân thủ và audit nội bộ**	Luật Thanh tra, Kiểm toán nội bộ; NĐ 13 (ktra 1 lần/năm bởi Bộ CA có thể) [35]	Thiết lập cơ chế **tự kiểm tra, đánh giá** việc tuân thủ: – **Đánh giá nội bộ định kỳ:** Ít nhất hàng năm, **bộ phận kiểm toán nội bộ hoặc tổ chuyên trách** tiến hành kiểm tra việc thực hiện các kiểm soát đề ra. Ví dụ: kiểm tra ngẫu nhiên xem DPIA có lập không khi phát sinh chuyển dữ liệu mới; kiểm tra cấu hình cloud có lệch chuẩn không; đối chiếu log xem retention có tuân thủ. – **Kiểm tra đột xuất khi có sự cố:** Sau mỗi sự cố lớn (vd lộ dữ liệu), tiến hành audit nguyên nhân, từ đó đánh giá lại tuân thủ quy	*Báo cáo kiểm toán nội bộ:* tài liệu liệt kê các kiểm soát đã chọn mẫu kiểm tra, phát hiện (nếu có) và khuyến nghị. *Checklist tuân thủ:* dạng excel theo dõi từng yêu cầu pháp lý – tình trạng tuân thủ (Comply/ Partial/Non) – bằng chứng – người chịu trách nhiệm. *Biên bản họp BLĐ:* cuộc họp xem xét kết quả audit, có quyết nghị về cải tiến nguồn lực, ngân sách nếu cần để khắc phục điểm yếu. *Chứng chỉ/giấy chứng nhận:* nếu có thuê đánh giá độc lập dẫn đến chứng nhận (vd ISO 27001) thì lưu chứng chỉ, báo cáo	**Kiểm toán nội bộ** (hoặc nếu không có, thì **bộ phận Rủi ro/ Compliance**) thực hiện đánh giá. **Ban lãnh đạo** nhận báo cáo và chỉ đạo các đơn vị khắc phục vấn đề. **Bộ phận IT/ATTT** phối hợp cung cấp thông tin, bằng chứng cho kiểm toán.	- Sử dụng **framework chuẩn** để audit: ví dụ bộ câu hỏi tham chiếu CSA Cloud Control Matrix, CIS Controls Cloud, hoặc checklist điều khoản luật VN. - Có thể thuê dịch vụ **đánh giá tuân thủ** của hãng tư vấn luật/công nghệ để có góc nhìn khách quan. - Nếu áp dụng tiêu chuẩn **ISO/IEC 27001**, đảm bảo đưa các kiểm soát liên quan cloud và luật VN vào tuyên bố áp dụng, để khi chứng nhận sẽ cover luôn phần này.

		trình nào chưa tốt, cập nhật. – **Báo cáo quản lý:** Tổng hợp kết quả giám sát (số sự cố, số phát hiện không tuân thủ) báo cáo Ban lãnh đạo và đề xuất cải tiến. – **Chuẩn bị cho kiểm tra bên ngoài:** Nếu cơ quan nhà nước (Bộ CA, Bộ TT&TT) tiến hành thanh tra, doanh nghiệp cần có sẵn tài liệu, bằng chứng (như bảng này liệt kê) để chứng minh tuân thủ. Doanh nghiệp nên chủ động thực hiện **kiểm toán độc lập** (ví dụ thuê công ty kiểm toán CNTT đánh giá compliance cloud) mỗi 2-3 năm,	đánh giá chứng nhận.

Nhóm/Yêu cầu	Nguồn luật tham chiếu	Mô tả biện pháp kiểm soát	Bằng chứng tuân thủ cần có	Trách nhiệm chính	Công cụ gợi ý
		vừa để chứng thực khách quan vừa luyện tập trước khi cơ quan chức năng kiểm tra.			

- **Quy trình quản lý sự cố & báo cáo**	NĐ 13 (thông báo vi phạm cho Bộ CA) [76] ; Luật ATTTM (phối hợp ứng cứu sự cố)	Định sẵn **quy trình quản lý sự cố an toàn thông tin** liên quan cloud, đảm bảo các bước: phát hiện, phân loại, ứng cứu, thông báo, hồi phục: – **Kênh báo cáo nội bộ:** Nhân viên phải biết cách báo ngay cho bộ phận CNTT/ ATTT khi phát hiện sự cố (ví dụ email phishing nghi ngờ, dữ liệu trên cloud bị xóa…). Thiết lập hotline hoặc hòm thư sự cố. – **Thông báo cơ quan NN:** Phân loại sự cố theo yêu cầu pháp luật: nếu sự cố **lộ dữ liệu cá nhân** số lượng lớn hoặc nhạy cảm, phải **thông báo**	*Quy trình/ quy chế sự cố:* văn bản chuẩn y bởi lãnh đạo, có lưu đồ xử lý sự cố ATTT, quy định thời gian từng bước (SLA nội bộ ví dụ trong 2h phải đánh giá mức độ, 24h báo cáo ban GĐ…). *Danh bạ liên hệ sự cố:* bảng thông tin liên hệ đội xử lý, cơ quan chức năng liên quan (A05 – Bộ CA, VNCERT). *Bản sao thông báo sự cố:* nếu đã từng thông báo Bộ CA hoặc khách hàng, lưu lại nội dung và thời gian gửi. *Báo cáo sự cố:* ví dụ báo cáo phân tích một vụ lộ lọt dữ liệu trên cloud, gồm diễn biến, dữ liệu ảnh hưởng, biện pháp khắc	**CSIRT (đội ứng cứu sự cố)** dẫn dắt xử lý khi có vụ việc. **DPO/Pháp chế** phụ trách quyết định việc thông báo cơ quan NN và soạn thảo nội dung pháp lý. **Marketing/ PR** (nếu cần) hỗ trợ soạn thông báo khách hàng, báo chí. **Lãnh đạo cao nhất (CEO)** phê duyệt thông báo ra bên ngoài để đảm bảo nhất quán.	- Áp dụng **playbook sự cố** theo tiêu chuẩn như NIST 800-61 hoặc ISO 27035 để không sót bước. - Sử dụng công cụ **ticket** (Jira Service Desk, ServiceNow) để quản lý sự cố từ lúc mở đến đóng, gán trách nhiệm và thời gian. - Tham gia **mạng lưới chia sẻ sự cố** (như diễn đàn VNISA, FB cộng đồng IT) để cập nhật thông tin sự cố mới, IOC (indicator) liên quan nhằm phản ứng nhanh.

		cho Bộ CA kịp thời (có thể thông qua đầu mối đã chỉ định) [76]. Nếu sự cố nghiêm trọng ảnh hưởng dịch vụ công cộng, có thể phải báo cho Trung tâm ứng cứu sự cố quốc gia (VNCERT/CSIRT) theo Luật ATTTM. – **Thông báo khách hàng/cá nhân bị ảnh hưởng:** Xem xét trường hợp cần thông báo cho chủ thể dữ liệu (dù luật VN chưa bắt buộc, nhưng là thông lệ tốt tránh mất niềm tin và nguy cơ pháp lý về sau). – **Điều tra và khắc phục:** Có quy trình điều tra nguyên nhân gốc rễ (root cause analysis) sau sự cố, lập	phục, người phụ trách, ngày hoàn thành khắc phục.

Nhóm/Yêu cầu	Nguồn luật tham chiếu	Mô tả biện pháp kiểm soát	Bằng chứng tuân thủ cần có	Trách nhiệm chính	Công cụ gợi ý
		báo cáo sự cố, cập nhật biện pháp phòng ngừa tái diễn. – **Bài học kinh nghiệm:** Tổ chức họp rút kinh nghiệm và điều chỉnh chính sách nếu cần.			
Contracts & Legal Terms					

- **Ký kết Thỏa thuận xử lý dữ liệu (DPA) với CSP**	NĐ 13 (Điều 39.1) – cần hợp đồng xử lý dữ liệu [24] ; TT 09/2020 NHNN – quy định nội dung hợp đồng cloud [62] [63]	Đảm bảo có **phụ lục hợp đồng về bảo vệ dữ liệu** (Data Processing Addendum) ký với CSP, bao gồm các điều khoản tối thiểu: – **Mục đích, phạm vi xử lý:** CSP chỉ được xử lý dữ liệu khách hàng cho mục đích cung cấp dịch vụ, không được dùng cho mục đích riêng hay chia sẻ cho bên thứ ba nếu không được phép [25] . – **Bảo mật và an ninh:** CSP phải áp dụng các biện pháp bảo vệ dữ liệu theo tiêu chuẩn tốt, thông báo ngay cho khách hàng nếu xảy ra vi phạm an ninh. – **Địa điểm lưu trữ:** Nêu rõ dữ	*Bản hợp đồng/DPA đã ký:* (thường dạng PDF/ Doc) có chữ ký hai bên. Các điều khoản chính được highlight để đối chiếu đủ nội dung yêu cầu. *Phê duyệt pháp chế:* chữ ký/ý kiến của bộ phận pháp chế trên hợp đồng thể hiện đã rà soát điều khoản về dữ liệu. *Bản cam kết riêng (nếu có):* trong trường hợp CSP không sửa được hợp đồng tiêu chuẩn, có thể có email hoặc văn bản cam kết riêng về một số điểm (lưu giữ tại hồ sơ pháp lý).	**Phòng Pháp chế** chịu trách nhiệm soạn thảo/đàm phán điều khoản hợp đồng về dữ liệu. **Bộ phận CNTT/ATTT** hỗ trợ cung cấp yêu cầu kỹ thuật (ví dụ muốn data center tại VN). **Người đại diện pháp luật** ký hợp đồng cuối cùng.	- Sử dụng **mẫu DPA tiêu chuẩn** có tham chiếu GDPR và tùy chỉnh bổ sung cho phù hợp NĐ 13 (vì nhiều CSP quốc tế có sẵn DPA cho GDPR, cần bổ sung yêu cầu VN như đăng ký A05, thông báo sự cố cho A05...). - Nếu CSP lớn khó đàm phán, tập trung thương thảo qua **điểm liên hệ địa phương của CSP** (đại diện kinh doanh tại VN) để họ hiểu tầm quan trọng và xin ý kiến từ trụ sở chính.

		liệu sẽ được lưu ở đâu (region nào), cam kết không chuyển dữ liệu ra ngoài region đó nếu chưa được sự đồng ý/hay đáp ứng yêu cầu pháp luật. Với CSP nội địa, yêu cầu dữ liệu ở trên lãnh thổ VN trừ khi khách hàng cho phép khác (phòng trường hợp CSP có DC nước ngoài). – **Quyền yêu cầu audit:** Khách hàng hoặc kiểm toán do khách hàng ủy quyền có quyền kiểm tra việc tuân thủ của CSP (có thể thông qua chứng chỉ, báo cáo bảo mật thay thế nếu CSP không cho audit trực tiếp). – **Hỗ trợ tuân thủ pháp**

Nhóm/Yêu cầu	Nguồn luật tham chiếu	Mô tả biện pháp kiểm soát	Bằng chứng tuân thủ cần có	Trách nhiệm chính	Công cụ gợi ý
		luật: CSP cam kết hợp tác nếu khách hàng cần cung cấp thông tin cho cơ quan VN, hoặc hỗ trợ khách thực hiện yêu cầu của chủ thể dữ liệu (ví dụ xóa dữ liệu cá nhân). – **Bảo mật thông tin khách hàng:** Thường kèm thỏa thuận không tiết lộ (NDA), CSP không được tiết lộ việc khách lưu trữ loại dữ liệu nào (trừ theo yêu cầu pháp luật). (*Những điều khoản cụ thể hơn sẽ liệt kê ở phần D – Checklist hợp đồng*).			

- **Kiểm soát các điều khoản quan trọng khác trong hợp đồng cloud**	Luật VT 2023 (quyền nghĩa vụ DN cung cấp cloud) [78] [79]; Thông lệ quốc tế (Cloud SLA, uptime commitment)	Ngoài DPA, hợp đồng dịch vụ cloud (MSA – Master Service Agreement) cần được xem xét kỹ: – **Uptime & SLA phạt vi phạm:** Đảm bảo có điều khoản về **mức độ dịch vụ (SLA)** – ví dụ uptime 99.9%. Quy định rõ mức bồi thường hoặc credit nếu CSP vi phạm SLA. – **Trách nhiệm về nội dung:** Luật Viễn thông 2023 quy định CSP **không chịu trách nhiệm về nội dung thông tin của người dùng trừ khi luật khác có quy định** [78]. Điều này có lợi cho CSP, nhưng khách hàng cũng nên có điều khoản	*Checklist pháp lý nội bộ:* tài liệu do pháp chế đánh dấu từng điều khoản quan trọng có trong hợp đồng hay chưa, nếu khác thường thì ghi nhận để lãnh đạo duyệt. *Biên bản đàm phán:* nếu có cuộc họp/call thương thảo, lưu biên bản các điểm đã thống nhất sẽ chỉnh sửa. *Bản hợp đồng cuối cùng:* phần Điều khoản dịch vụ và Phụ lục kèm (SLA, Support Policy...). Các điều khoản nêu trên highlight để đối chiếu. *Thư xác nhận của CSP:* trường hợp CSP không sửa HĐ chung nhưng có gửi thư/ email đảm	**Phòng Pháp chế** chủ trì rà soát hợp đồng. **Phòng Mua sắm/IT** tham gia đàm phán các điều khoản kỹ thuật, thương mại. **Lãnh đạo cấp cao** (CFO, CEO) tham gia nếu đàm phán các điều khoản quan trọng bồi thường, giới hạn trách nhiệm cần quyết định.	- Chuẩn bị sẵn **Cloud Contract Checklist** (mục D) và dùng khi review bất kỳ hợp đồng cloud nào. - Tham khảo **hợp đồng mẫu** của các đơn vị công (nếu có) hoặc kinh nghiệm từ các diễn đàn pháp lý CNTT để biết mức nào là chấp nhận được. - Sử dụng **dịch vụ tư vấn bên ngoài** (luật sư CNTT) cho các hợp đồng giá trị/rủi ro cao để đảm bảo không bỏ sót chi tiết bất lợi.

		trong hợp đồng rằng **khách hàng tự chịu trách nhiệm nội dung**, CSP hỗ trợ khi có yêu cầu gỡ bỏ từ cơ quan chức năng. – **Bảo vệ quyền sở hữu dữ liệu:** Khẳng định trong hợp đồng: *toàn bộ dữ liệu do khách hàng đưa lên và dữ liệu phát sinh thuộc sở hữu của khách hàng* [62]. CSP chỉ giữ vai trò lưu giữ, không có quyền sở hữu hoặc dùng cho mục đích khác. – **Chuyển giao dữ liệu khi chấm dứt:** Điều khoản yêu cầu CSP **hỗ trợ chuyển giao dữ liệu** về cho khách hàng hoặc sang dịch vụ khác khi chấm	bảo một số yêu cầu (ví dụ “chúng tôi xác nhận sẽ xóa dữ liệu khách hàng theo yêu cầu trong 30 ngày”), thì lưu làm phụ lục.

	dứt, và **xóa vĩnh viễn dữ liệu khách hàng khỏi hệ thống** trong thời hạn nhất định (VD 30-60 ngày) [63]. Yêu cầu CSP xác nhận việc xóa xong (certificate of deletion). – **Bảo đảm tách biệt dữ liệu:** CSP cam kết kỹ thuật **cách ly dữ liệu khách hàng** (multi-tenancy isolation) – không để dữ liệu khách này "nhìn thấy" dữ liệu khách khác [63]. – **Bồi thường và giới hạn trách nhiệm:** Thương thảo mức **bồi thường thiệt hại** nếu CSP vi phạm nghĩa vụ bảo mật gây tổn thất (thường CSP giới hạn tổng trách

Nhóm/Yêu cầu	Nguồn luật tham chiếu	Mô tả biện pháp kiểm soát	Bằng chứng tuân thủ cần có	Trách nhiệm chính	Công cụ gợi ý
		nhiệm = phí dịch vụ 6-12 tháng; khách nên cố gắng nâng mức này hoặc có ngoại lệ nếu do lỗi cố ý của CSP). – **Chấm dứt do yêu cầu pháp lý:** Thêm điều khoản nếu có sự kiện pháp lý bất khả kháng (ví dụ luật thay đổi cấm dùng cloud nước ngoài cho loại dữ liệu X), khách hàng có quyền chấm dứt hợp đồng trước hạn và CSP hoàn trả phí còn lại.			

D) Checklist hợp đồng cloud (Cloud Contract Clause Checklist)

Khi ký hợp đồng với nhà cung cấp cloud, doanh nghiệp cần đảm bảo các điều khoản hợp đồng bảo vệ quyền lợi và tuân thủ pháp luật. Bảng sau liệt kê các **chủ đề quan trọng**, điều khoản cần có, mục tiêu của điều khoản, dấu hiệu "red flag" nếu điều khoản bất lợi, và nguồn bằng chứng/tham chiếu liên quan.

Bảng: Checklist các điều khoản hợp đồng cloud cần lưu ý

Chủ đề	Điều khoản cần có	Mục tiêu	Red flags (Cảnh báo)	Evidence / Nguồn pháp lý
Quyền sở hữu dữ liệu khách hàng	*Data Ownership:* Xác định rõ *"Khách hàng sở hữu mọi dữ liệu do khách hàng đưa lên và dữ liệu được tạo ra trong quá trình sử dụng dịch vụ."*	Đảm bảo rằng thông tin, dữ liệu của khách hàng trên cloud hoàn toàn thuộc về khách hàng, CSP không có quyền sở hữu hay sử dụng ngoài mục đích cung cấp dịch vụ. Điều này phù hợp NĐ 13 (bên xử lý không được quyết định mục đích) và quy định NHNN: *"dữ liệu phát sinh... là tài sản của ngân hàng."* 62 .	– Hợp đồng im lặng về quyền sở hữu dữ liệu, hoặc có câu mập mờ kiểu "CSP có quyền sử dụng dữ liệu để cải thiện dịch vụ" – nguy cơ CSP khai thác dữ liệu cho mục đích riêng (data mining). – Điều khoản cho phép CSP giữ lại dữ liệu sau khi chấm dứt (trừ backup tạm thời) cũng đáng lo, vi phạm nguyên tắc khách hàng kiểm soát dữ liệu.	– **Hợp đồng/DPA đã ký** có mục "Ownership" hoặc "Customer Data" nêu khách hàng retains all right, title in Customer Data. – **Nguồn tham chiếu:** TT 09/2020 NHNN yêu cầu dữ liệu phát sinh thuộc tài sản NH 62 – áp dụng tương tự cho doanh nghiệp.

Chủ đề	Điều khoản cần có	Mục tiêu	Red flags (Cảnh báo)	Evidence / Nguồn pháp lý
Địa điểm lưu trữ & chuyển dữ liệu	*Data Residency:* Quy định nơi dữ liệu khách hàng được lưu trữ (VD: *"Dữ liệu sẽ được lưu tại trung tâm dữ liệu ở Singapore. CSP sẽ không di chuyển dữ liệu ra ngoài địa điểm này nếu không được khách hàng chấp thuận bằng văn bản."*).	Đáp ứng yêu cầu **định vị dữ liệu** – khách hàng biết dữ liệu ở đâu để tuân thủ luật (Luật ANM đòi lưu tại VN trong TH nhất định). Điều khoản này ngăn CSP tự ý chuyển dữ liệu sang quốc gia khác (phổ biến khi CSP cân bằng tải). Nếu cần chuyển, phải được sự đồng ý hoặc tuân thủ thủ tục (DPIA...).	– CSP từ chối cam kết vị trí lưu trữ cụ thể, chỉ nói chung chung "có thể lưu ở bất kỳ DC nào trên toàn cầu để tối ưu". Đây là red flag vì khách hàng mất kiểm soát, có thể vi phạm NĐ 13 do dữ liệu chuyển quốc gia mà không biết. – Điều khoản cho phép CSP sao lưu tất cả dữ liệu sang DC khác (ngoài VN) mà không cần hỏi – cũng nguy hiểm trừ phi khách hàng đã làm DPIA cho trường hợp đó.	– **Hợp đồng** phần "Data Location" nêu rõ tên quốc gia hoặc vùng địa lý. Nếu hợp đồng chính không có, có thể là cấu hình trong điều khoản kỹ thuật (ví dụ: dịch vụ ở region X). – **Nguồn pháp lý:** Luật ANM 2018 yêu cầu lưu tại VN với một số dữ liệu [1] ; NĐ 13 yêu cầu quản lý chuyển dữ liệu ra ngoài [29] .

Chủ đề	Điều khoản cần có	Mục tiêu	Red flags (Cảnh báo)	Evidence / Nguồn pháp lý
Bảo mật và biện pháp an ninh	*Security Measures:* CSP cam kết sẽ triển khai các biện pháp bảo mật phù hợp (ví dụ: mã hóa, kiểm soát truy cập, chứng chỉ ISO 27001), và tuân thủ luật ATTT, luật bảo vệ DL. Có thể liệt kê hoặc dẫn chiếu tài liệu "Security Policy" của CSP.	Ràng buộc **trách nhiệm an toàn thông tin** của CSP. Khách hàng có căn cứ yêu cầu CSP duy trì chứng chỉ, thông báo nếu có thay đổi biện pháp bảo mật quan trọng. Mục tiêu để CSP không thể phủi trách nhiệm hoàn toàn (dù thực tế phần bảo mật chia sẻ). Luật VT 2023 đòi CSP tuân thủ ATTT, bảo vệ DL cá nhân [73], nên nên đưa thành điều khoản hợp đồng.	– Điều khoản đẩy hết trách nhiệm bảo mật cho khách hàng (câu thường gặp: "Customer is responsible for security of their content."). Mặc dù mô hình chia sẻ trách nhiệm có phần khách hàng, nhưng nếu CSP không nhận trách nhiệm gì -> rủi ro. – CSP không nhắc gì tới tuân thủ luật (ANM, PDP) – có thể họ chưa sẵn sàng hỗ trợ, khách hàng sẽ khó yêu cầu sau này.	– **Hợp đồng/DPA** có mục "Security" nêu CSP duy trì "appropriate technical and organizational measures" để bảo vệ dữ liệu (theo chuẩn như ISO 27001, SOC2...). – **Chứng chỉ bảo mật** CSP cung cấp (ISO, SOC2) làm phụ lục tham chiếu. – **Nguồn:** NĐ 13 Điều 39.3 yêu cầu CSP thực hiện đủ biện pháp bảo vệ DL [26]; TT 09 NHNN đòi CSP có chứng chỉ ATTT [62].

Chủ đề	Điều khoản cần có	Mục tiêu	Red flags (Cảnh báo)	Evidence / Nguồn pháp lý
Thông báo vi phạm và sự cố	*Breach Notification:* Yêu cầu CSP phải thông báo cho khách hàng **ngay lập tức** (hoặc trong thời hạn rất ngắn, ví dụ 24-48h) nếu phát hiện sự cố bảo mật liên quan dữ liệu khách hàng.	Để khách hàng có thể **chủ động phản ứng**, tuân thủ nghĩa vụ báo cơ quan NN (NĐ 13 yêu cầu thông báo Bộ CA "kịp thời" khi có vi phạm). Nếu CSP chậm báo, khách hàng mất thời gian quý giá ứng cứu và có thể bị coi là chậm trễ báo cáo.	– Hợp đồng thiếu điều khoản này, hoặc nói CSP "sẽ nỗ lực hợp lý để thông báo trong thời gian kịp thời". Ngôn ngữ mơ hồ có thể khiến CSP trì hoãn báo cáo (như vụ một số hãng giấu breach). – CSP giới hạn loại sự cố phải thông báo chỉ khi "ảnh hưởng nghiêm trọng dịch vụ" – có thể bỏ sót sự cố lộ dữ liệu (vì dịch vụ vẫn chạy).	– **Hợp đồng/DPA** mục "Security Incident" có quy định thời hạn (ví dụ: "within 24 hours of confirmation of a data breach, Provider shall notify Customer..."). – **Quy trình liên hệ sự cố** đính kèm: thông tin đầu mối 24/7 của CSP để báo sự cố. – **Nguồn:** NĐ 13 Điều 42 yêu cầu tổ chức thông báo Bộ CA ngay khi có vi phạm DL [80] – muốn thế cần CSP báo sớm.
Kiểm toán và giám sát	*Audit Rights:* Khách hàng (hoặc kiểm toán thứ ba được khách uỷ quyền) có quyền **kiểm tra** mức độ tuân thủ của CSP đối với các điều khoản an ninh, bảo vệ dữ liệu. Thực tế thường: CSP cung cấp báo cáo độc lập (ISO/SOC) thay cho audit trực tiếp.	Đảm bảo khách hàng có **tầm nhìn minh bạch** vào hoạt động của CSP liên quan dữ liệu mình. Nếu luật yêu cầu chứng minh (VD cơ quan đòi bằng chứng CSP giữ an toàn), khách hàng cần quyền này để thu thập. Cũng là cách gây áp lực để CSP duy trì chứng chỉ, không lơ là.	– CSP hạn chế quá mức: chỉ cho phép audit nếu luật bắt buộc, hoặc tính phí rất cao cho mỗi lần audit, hoặc chỉ cho audit phần hạ tầng chung chứ không cho xem log liên quan khách hàng. – Không cung cấp được báo cáo độc lập cũng là red flag – CSP kém uy tín hoặc non trẻ.	– **Điều khoản Audit** trong DPA: thường ghi "Customer may audit compliance up to 1x per year, with 30 days notice, non-intrusive... or accept independent audit reports." – **Báo cáo SOC2/ISO**: CSP cung cấp bản tóm tắt hoặc chứng chỉ, khách hàng lưu làm bằng chứng đã thực hiện quyền giám sát. – **Nguồn:** Luật VT 2023 cho phép quản lý "nhẹ" qua công bố chất lượng [81], nhưng khách hàng doanh nghiệp vẫn cần audit chi tiết cho an tâm.

Chủ đề	Điều khoản cần có	Mục tiêu	Red flags (Cảnh báo)	Evidence / Nguồn pháp lý
Chuyển tiếp cho bên thứ ba (Sub-processor)	*Subprocessor clause:* CSP phải liệt kê hoặc **thông báo** trước danh sách các bên thứ ba sẽ tham gia xử lý dữ liệu khách hàng (ví dụ dịch vụ hỗ trợ, nhà thầu phụ). Bất kỳ thay đổi (thêm sub-processor mới) phải báo cho khách hàng và cho phép khách hàng phản đối nếu ảnh hưởng nghiêm trọng.	Đảm bảo **minh bạch** về việc ai thực sự có thể truy cập dữ liệu. Nhiều CSP dùng nhà thầu phụ (VD thuê data center của bên khác, thuê support). Điều khoản này giúp khách hàng biết và đánh giá rủi ro chuỗi cung ứng. Cũng đáp ứng NĐ 13, bên thứ ba chỉ được xử lý nếu được phép [23].	– CSP không cung cấp thông tin sub-processor, hoặc cho rằng danh sách "bí mật". Điều này không phù hợp thông lệ (các CSP lớn đều có trang web liệt kê sub). – CSP giữ quyền thêm bất kỳ sub nào bất kỳ lúc nào mà không cần báo – khách hàng mất kiểm soát, có thể đột nhiên dữ liệu mình do một công ty khác xử lý (có rủi ro pháp lý nếu công ty đó ở nước khác).	– **Phụ lục Sub-processor:** danh sách tên các công ty, loại dịch vụ họ cung cấp, quốc gia. – **Điều khoản thông báo:** ví dụ "CSP sẽ thông báo ít nhất 30 ngày trước khi bổ sung sub-processor mới, khách hàng có quyền phản đối vì lý do hợp lý. Nếu không đạt đồng thuận, khách có thể chấm dứt HĐ." – **Nguồn:** NĐ 13: bên thứ ba chỉ xử lý nếu được cho phép [23].

Chủ đề	Điều khoản cần có	Mục tiêu	Red flags (Cảnh báo)	Evidence / Nguồn pháp lý
Xóa dữ liệu & trả dữ liệu khi chấm dứt	*Data Return/Deletion:* Quy định quy trình khi hợp đồng kết thúc: CSP sẽ **trả lại tất cả dữ liệu** cho khách hàng (ví dụ cung cấp bản sao, hoặc cho tải xuống), sau đó **xóa vĩnh viễn dữ liệu** trên hệ thống CSP trong thời hạn X ngày. Có thể yêu cầu chứng nhận bằng văn bản việc xóa hoàn tất.	Đảm bảo **quyền "được quên"** cho dữ liệu khách hàng. Phù hợp NĐ 13 (chấm dứt xử lý phải xoá/ trả dữ liệu) [27] . Ngăn việc CSP còn lưu giữ bản sao dữ liệu sau khi khách hàng rời đi (trừ backup lưu cache tạm thì phải xóa sớm). Giảm nguy cơ lộ dữ liệu về sau.	– Hợp đồng không nhắc tới, mặc định CSP có thể vẫn giữ dữ liệu (một số CSP có chính sách lưu backup 90 ngày, nếu không cam kết xóa sớm -> dữ liệu nằm đó ngoài tầm kiểm soát). – CSP tính phí quá đáng để trả dữ liệu (nhiều dịch vụ cho tải miễn phí, nhưng nếu có phí, cần thoả thuận rõ mức hợp lý). – Không có cam kết thời gian xóa – dữ liệu có thể tồn tại mãi.	– **Điều khoản Return/Deletion:** ví dụ "Upon termination, Provider shall make available to Customer all Customer Data in X format. Within 30 days thereafter, Provider shall permanently delete or overwrite all Customer Data from its systems, except as required by law, and provide written certification upon request." – **Nguồn:** NĐ 13 Điều 39.5 yêu cầu bên xử lý xóa/trả dữ liệu sau khi kết thúc [27] ; TT 09 NHNN cũng yêu cầu tương tự [63] .

Chủ đề	Điều khoản cần có	Mục tiêu	Red flags (Cảnh báo)	Evidence / Nguồn pháp lý
Bồi thường và giới hạn trách nhiệm	*Liability and Indemnification:* Điều khoản quy định mức độ **trách nhiệm pháp lý** của CSP nếu vi phạm hợp đồng, đặc biệt nếu do lỗi CSP làm lộ dữ liệu hay gián đoạn dịch vụ gây thiệt hại cho khách hàng, CSP sẽ bồi thường bao nhiêu. Thường CSP giới hạn tổng trách nhiệm (cap) = X tháng phí dịch vụ, và loại trừ thiệt hại gián tiếp. Khách hàng cần xem mức đó có chấp nhận được không.	Đảm bảo CSP có **động lực tuân thủ**. Nếu không có ràng buộc tài chính, CSP có thể lơ là. Dù khó buộc CSP nhận trách nhiệm lớn, khách nên cố gắng: – Yêu cầu **bồi thường với vi phạm bảo mật**: nếu lộ data do lỗi CSP (ví dụ cấu hình sai), CSP phải chịu các chi phí thông báo, khắc phục… – Mức trần trách nhiệm: cố đàm phán cao hơn giá trị hợp đồng nếu có thể, hoặc **không giới hạn** trong trường hợp cố ý, vi phạm pháp luật nghiêm trọng.	– CSP đưa điều khoản miễn trừ tối đa, ví dụ "CSP not liable for any damages" – rất bất lợi, khách hàng không có đòn bẩy. – Mức bồi thường quá thấp (vd 1 tháng phí), không thấm vào đâu so với thiệt hại tiềm tàng do sự cố. – Không có ngoại lệ cho trường hợp vi phạm nghĩa vụ bảo mật hay pháp lý – tức là ngay cả khi CSP vi phạm luật, khách cũng không đòi thêm được.	– **Điều khoản trách nhiệm**: ví dụ "CSP's total liability shall not exceed 12 months of fees. However, this cap shall not apply to breach of confidentiality or data protection obligations, for which CSP will indemnify Customer for direct losses." – Nếu không đàm phán được, ít nhất lưu ý trong **đánh giá rủi ro nội bộ**: chấp nhận rủi ro phần vượt quá. – **Nguồn:** Luật VT 2023 vẫn cho CSP không chịu trách nhiệm nội dung người dùng [78], nhưng về bảo mật hợp đồng vẫn thỏa thuận.

Chủ đề	Điều khoản cần có	Mục tiêu	Red flags (Cảnh báo)	Evidence / Nguồn pháp lý
Luật áp dụng và giải quyết tranh chấp	*Governing Law & Dispute Resolution:* Xác định luật nước nào điều chỉnh hợp đồng và cách thức giải quyết tranh chấp (tòa án VN hay trọng tài quốc tế…). Với cloud phục vụ tại VN, khách hàng thường mong muốn **luật Việt Nam** và tòa/ trọng tài VN để dễ bảo vệ quyền lợi.	Tránh trường hợp phải theo kiện ở nước ngoài với chi phí cao và bất lợi ngôn ngữ. Đảm bảo hợp đồng chịu luật VN cũng thúc đẩy CSP tuân thủ luật VN (ANM, PDP…) vì nếu không họ sẽ vi phạm hợp đồng.	– CSP kiên quyết luật nước ngoài (như luật Singapore/Anh) và giải quyết ở tòa nước ngoài – khách hàng phải cân nhắc rủi ro: nếu có tranh chấp, mình phải theo sân chơi của họ. – Nếu khách hàng rất cần dịch vụ và đành chấp nhận luật nước ngoài, xem xét chọn **trọng tài trung lập** (ICC, SIAC) để ít ra tránh toà án thiên vị CSP.	– **Điều khoản Governing Law:** "This Agreement shall be governed by the laws of Vietnam. Disputes shall be subject to jurisdiction of courts of Vietnam." Hoặc nếu thỏa hiệp: "luật Singapore, tranh chấp giải quyết tại SIAC". – Khách hàng cần **tham vấn ý kiến pháp lý** khi chấp nhận luật khác, để hiểu ảnh hưởng (ví dụ luật Mỹ về discovery, v.v.). – **Nguồn:** Không trực tiếp từ luật nào cho hợp đồng dân sự, nhưng nguyên tắc chung nếu dịch vụ cung cấp chủ yếu tại VN, áp dụng luật VN là hợp lý.

E) Các tùy chọn kiến trúc Cloud theo mức độ rủi ro

Dựa trên khẩu vị rủi ro và yêu cầu tuân thủ, tổ chức có thể chọn kiến trúc triển khai cloud phù hợp. Dưới đây là một số **phương án kiến trúc từ thận trọng đến linh hoạt**, cùng đánh giá khi nào nên áp dụng, điều kiện tuân thủ kèm theo, ưu nhược điểm và rủi ro còn lại:

Bảng: Lựa chọn kiến trúc Cloud theo mức độ rủi ro tuân thủ

Tùy chọn kiến trúc	Mô tả	Sử dụng khi	Điều kiện tuân thủ kèm theo	Ưu điểm	Hạn chế & Rủi ro còn lại
1. On-Premises / Private Cloud nội bộ (Truyền thống nhất)	Doanh nghiệp tự xây dựng hạ tầng CNTT tại chỗ hoặc private cloud nội bộ. Dữ liệu lưu trữ và xử lý **100% trong hệ thống do doanh nghiệp kiểm soát**, không phụ thuộc bên thứ ba.	– Dữ liệu cực kỳ nhạy cảm: bí mật nhà nước, bí mật kinh doanh cốt lõi, dữ liệu tài chính quan trọng chưa sẵn sàng đưa ra. – Tổ chức có quy mô lớn đủ nguồn lực vận hành trung tâm dữ liệu riêng, hoặc có yêu cầu pháp lý đặc thù buộc hạ tầng độc lập (một số cơ quan an ninh, quốc phòng).	– Tuân thủ dễ dàng: dữ liệu nằm trong lãnh thổ, không phải lo thủ tục chuyển dữ liệu. Chỉ cần đảm bảo tuân thủ các quy định an toàn (Luật ATTTM) như bình thường. – Nếu xử lý thông tin cấp độ 4-5: cần phê duyệt phương án bảo đảm ATTT với cơ quan QLNN (theo NĐ 85) nhưng do hệ thống nội bộ, phê duyệt dễ hơn so với dùng public cloud.	– **Chủ quyền dữ liệu:** Kiểm soát hoàn toàn, đáp ứng yêu cầu nội địa hóa (Luật ANM) một cách tuyệt đối. – **Bảo mật cao nhất:** Không phụ thuộc bên ngoài, giảm nguy cơ truy cập trái phép bởi nhân viên bên thứ ba. – **Tùy biến tuyệt đối:** Doanh nghiệp tự quyết định kiến trúc, không bị giới hạn bởi cấu hình nhà cung cấp.	– **Chi phí đầu tư lớn:** Xây dựng DC, mua server, thiết bị mạng, an ninh... tốn kém vốn đầu tư và chi phí vận hành (nhân sự, điện, bảo trì). – **Thiếu linh hoạt mở rộng:** Mua sắm theo chu kỳ, khó tăng giảm nhanh theo nhu cầu như cloud. – **Cập nhật công nghệ chậm:** Dễ lạc hậu nếu không đầu tư thường xuyên. – **Rủi ro còn lại:** Nếu nội bộ vận hành yếu, nguy cơ sự cố do thiếu kinh nghiệm. Không có SLA đảm bảo như dịch vụ cloud (hoàn toàn tự chịu). Ngoài ra, nếu thiết kế sai, vẫn có thể bị tấn công (on-prem không mặc định an toàn hơn cloud nếu không được bảo vệ tốt).

Tùy chọn kiến trúc	Mô tả	Sử dụng khi	Điều kiện tuân thủ kèm theo	Ưu điểm	Hạn chế & Rủi ro còn lại
2. Cloud riêng do nhà cung cấp trong nước vận hành (Vietnam Private Cloud)	Thuê dịch vụ **Private Cloud từ CSP Việt Nam**. CSP thiết lập một hạ tầng cloud **dành riêng** cho khách hàng (ví dụ một vùng tài nguyên tách biệt vật lý hoặc logic), đáp ứng yêu cầu riêng về bảo mật. Dữ liệu được đảm bảo nằm tại các DC ở Việt Nam của CSP.	– Doanh nghiệp muốn lợi ích linh hoạt của cloud nhưng vẫn phải bảo đảm dữ liệu không ra nước ngoài. – Có thể áp dụng cho cơ quan nhà nước theo yêu cầu "Cloud trong nước" của Chính phủ. – Trường hợp doanh nghiệp ngành tài chính muốn cloud nhưng NHNN yêu cầu hạ tầng đặt tại VN và do đối tác VN quản lý (dễ kiểm tra).	– CSP phải chứng minh đáp ứng tiêu chí an toàn (theo CV 1145/BTTTT: DC Tier III, ISO 27001, sẵn sàng kiểm tra cấp độ 4...). Khách hàng có thể yêu cầu đánh giá tiền kiểm. – Hợp đồng cần ràng buộc CSP về việc dữ liệu **không rời khỏi VN**, tuân thủ lệnh cơ quan VN (theo Luật ANM). – Khách hàng có thể cần xin chấp thuận cơ quan chủ quản (ví dụ Bộ chủ quản với đơn vị nhà nước) trước khi thuê cloud.	– **Tuân thủ dữ liệu tốt:** Dữ liệu ở VN, dưới pháp luật VN – đáp ứng yêu cầu nội địa hóa, thuận lợi cho thanh tra (cơ quan có thể trực tiếp đến DC kiểm tra). – **Quản trị dễ hơn on-prem:** Không phải tự vận hành vật lý, tận dụng chuyên môn CSP. – **Tùy biến bảo mật:** Private cloud có thể yêu cầu cấu hình đặc thù (VD: dedicate firewall, zone riêng), an tâm hơn multi-tenant công cộng.	– **Chi phí cao hơn public cloud thông thường:** Private cloud dành riêng thường đắt, có khi xấp xỉ vận hành on-prem. – **Mất một phần chủ động:** Phụ thuộc CSP nội địa – nếu CSP năng lực kém, có thể vận hành lỗi. Tuy nhiên rủi ro này giảm nếu chọn CSP lớn, uy tín (như Viettel, VNPT). – **Khả năng mở rộng hạn chế:** Private cloud có giới hạn tài nguyên nhất định cam kết cho khách; muốn mở rộng nhiều có thể cần hợp đồng thêm. – **Rủi ro còn lại:** Nếu CSP bị sự cố trên diện rộng (VD mất điện, cháy DC) – mặc dù dữ liệu trong nước, doanh nghiệp vẫn bị ảnh hưởng như dùng public cloud.

3. Hybrid Cloud (kết hợp on-prem và public cloud)	Doanh nghiệp triển khai mô hình **kết hợp**: một số hệ thống/dữ liệu vẫn chạy on-prem hoặc private cloud, một số ít nhạy cảm hơn chạy trên public cloud (có thể là cloud nước ngoài). Hai bên được kết nối tích hợp (qua VPN, MPLS). Thường dùng on-prem cho data tier, cloud cho web/app tier.	– Khi tổ chức có hạ tầng hiện hữu và muốn tận dụng, đồng thời hưởng lợi cloud cho phần tải biến động. – Dữ liệu nào luật cấm ra nước ngoài thì giữ on-prem; phần không nhạy cảm xử lý trên cloud. – Trường hợp phổ biến: cơ sở tài chính giữ CSDL khách hàng tại chỗ, dùng cloud cho ứng dụng phân tích, web scale-out.	– Phân định rõ **phạm vi dữ liệu**: cái gì lên cloud, cái gì không. Dựa theo **Data Classification** (phải có output phần C). – Cần thiết kế **kênh truyền an toàn** giữa on-prem và cloud (mạng riêng ảo, mã hóa) để dữ liệu di chuyển không bị nghe lén. – Có cơ chế **đồng bộ tuân thủ**: ví dụ log cloud đẩy về SIEM on-prem; tài khoản AD đồng bộ lên cloud. – Đáp ứng cả yêu cầu on-prem (theo NĐ 85…) lẫn cloud (DPIA nếu phần cloud có dữ liệu cá nhân ra nước ngoài).	**– Tối ưu cái tốt nhất của hai bên:** giữ được dữ liệu nhạy cảm “gần nhà”, đồng thời mở rộng năng lực tính toán khi cần với cloud (giảm chi phí đầu tư thừa). – **Linh hoạt pháp lý:** Dễ tuân thủ luật vì có thể điều chỉnh: nếu quy định mới cấm loại dữ liệu X ra nước ngoài, có thể kéo X về on-prem, phần khác vẫn cloud. – **Độ sẵn sàng cao:** Hạ tầng kép, nếu cloud gặp vấn đề có thể chuyển workload về on-prem tạm thời (nếu đã chuẩn bị).	**– Độ phức tạp cao:** Quản lý hai môi trường khác biệt, đòi hỏi kỹ năng đa dạng (nhân sự phải thạo cả quản trị hệ thống truyền thống và cloud). – **Chi phí tích hợp:** Thiết lập kênh truyền riêng (leased line/VPN) và công cụ quản lý chung (hybrid monitoring) tốn kém. – **Độ trễ và trải nghiệm:** Nếu ứng dụng phân tách (DB on-prem, app trên cloud) có thể gặp độ trễ, ảnh hưởng hiệu năng nếu kết nối mạng không đủ tốt. – **Rủi ro còn lại:** Nếu không quản lý tốt, có thể **rò rỉ dữ liệu từ on-prem sang cloud** (nhân viên tiện sử dụng cloud luôn cho dữ liệu cấm). Cần kỷ luật và giám sát. Ngoài ra, đội vận hành có thể bị quá tải do song song hai hệ thống.

4. Public Cloud tại Việt Nam (Region nội địa hoặc CSP nội)	Sử dụng dịch vụ **Public Cloud nhưng đặt tại data center ở Việt Nam**. Ví dụ: Google Cloud mở region tại Hà Nội (giả định), AWS mở region TP.HCM, hoặc dùng luôn cloud của CSP Việt (Viettel Cloud, VNG Cloud) theo mô hình multi-tenant công cộng.	– Muốn lợi ích public cloud (chi phí theo nhu cầu, dịch vụ phong phú) nhưng cũng đảm bảo **dữ liệu ở VN** vì lý do tuân thủ hoặc hiệu năng. – Phù hợp cho ứng dụng không quá nhạy cảm, nhưng dữ liệu yêu cầu độ trễ thấp (phục vụ người dùng VN) và muốn tránh rủi ro đứt cáp quốc tế. – Tổ chức có chính sách nội bộ yêu cầu dùng nhà cung cấp dịch vụ trong nước nếu có thể (ưu tiên "Make in Vietnam").	– Dù data ở VN, vẫn cần **điều khoản hợp đồng** ràng buộc CSP không di chuyển dữ liệu ra ngoài nếu không cần (phòng trường hợp backup sang DC phụ ở nước khác). – Kiểm tra **chứng chỉ tuân thủ** của region nội địa: region mới có thể chưa được các chứng chỉ quốc tế đầy đủ, nhưng ít nhất phải tuân thủ NĐ 53 (đặt hiện diện VN – đương nhiên có) và sẵn sàng hợp tác cơ quan chức năng (Luật ANM). – Thực hiện đánh giá như Vendor Due Diligence (phần C) đối với CSP nội địa: năng lực ATTT, quy trình. – Nếu CSP là công ty VN, ít phải lo thủ tục PDP cross-border, nhưng vẫn tuân thủ NĐ 13 chung.	– **Tuân thủ pháp lý dễ hơn cross-border:** Không cần DPIA vì dữ liệu không ra nước ngoài. Bộ CA cũng dễ yêu cầu cung cấp thông tin khi cần điều tra (CSP nội tuân lệnh nhanh). – **Hiệu năng cho người dùng VN:** Region trong nước cho độ trễ thấp, trải nghiệm tốt. – **Hỗ trợ tiếng Việt, hiểu luật:** CSP nội địa (hoặc region VN của hãng ngoại) có nhân sự hiểu bối cảnh VN, hỗ trợ khách hàng tuân thủ (ví dụ cung cấp hợp đồng tiếng Việt,	– **Hạn chế dịch vụ:** Region VN có thể ít dịch vụ hơn region lớn nước ngoài (đặc biệt các dịch vụ AI, Big Data mới đôi khi không triển khai ngay). – **Chi phí có thể cao hơn** region quốc tế do quy mô nhỏ hơn hoặc thiếu cạnh tranh. – **Rủi ro gián đoạn do hạ tầng VN:** DC nội địa vẫn có thể gặp sự cố hạ tầng (nguồn điện, thiên tai). Tuy tránh được đứt cáp quốc tế, nhưng nếu CSP chỉ có 1-2 DC trong nước, khả năng dự phòng địa lý thấp hơn so với dùng nhiều region global. – **Rủi ro pháp lý quốc tế:** Nếu CSP là công ty nước ngoài có hiện diện VN, họ vẫn chịu luật nước họ (ví dụ lệnh Cloud Act của Mỹ đòi dữ liệu từ chi nhánh VN). Khách hàng cần đánh giá trường hợp này – dù data ở VN nhưng có thể bị giao nộp ra ngoài theo kênh pháp lý khác.

Tùy chọn kiến trúc	Mô tả	Sử dụng khi	Điều kiện tuân thủ kèm theo	Ưu điểm	Hạn chế & Rủi ro còn lại
				tư vấn lưu trữ...).	

5. Public Cloud nước ngoài với mã hóa khóa do khách hàng giữ (Encrypted Foreign Cloud)	Lưu trữ và xử lý trên **public cloud nước ngoài**, nhưng áp dụng **mã hóa mạnh** ở mức ứng dụng; khóa giải mã do khách hàng nắm giữ (không lưu trên cloud). Ngay cả khi dữ liệu nằm trên cloud, CSP không thể đọc được nội dung.	– Dữ liệu có nhạy cảm (PII, tài chính) nhưng khách muốn tận dụng hạ tầng và dịch vụ tiên tiến của cloud nước ngoài. – Khách hàng chấp nhận làm DPIA và có phương án mã hóa để giảm thiểu rủi ro lộ dữ liệu. – Thường dùng trong ngành cần bảo mật cao: lĩnh vực tài chính sử dụng BYOK/HYOK, hoặc công ty đa quốc gia lưu dữ liệu khách hàng mã hóa để tuân thủ quy định mỗi nước.	– Đảm bảo **thiết kế mã hóa đầu-cuối** đúng cách: dữ liệu được mã hóa trước khi ghi lên cloud (client-side encryption) bằng khóa do khách giữ. – **Quản lý khóa an toàn:** Khóa được lưu trong HSM on-prem hoặc dịch vụ KMS tách biệt. Phải có backup khóa, và cơ chế thu hồi/đổi khi cần. – Vẫn phải **làm DPIA** và gửi Bộ CA (theo NĐ13) vì dù mã hóa, dữ liệu cá nhân vẫn được chuyển ra nước ngoài. Trong hồ sơ nêu rõ biện pháp mã hóa để Bộ CA đánh giá rủi ro thấp [32] . – Hợp đồng với CSP cần rõ nếu CSP nhận yêu cầu từ chính phủ nước ngoài đòi dữ liệu, họ phải thông báo khách hàng (để khách cho giải mã hoặc phản đối).	– **Tận dụng tối đa cloud**: có thể dùng các dịch vụ AI, Big Data trên hạ tầng mạnh mẽ toàn cầu mà vẫn giữ bí mật nội dung (trong chừng mực mã hóa cho phép). – **Bảo mật dữ liệu cao:** Ngay cả vi phạm cloud (như hacker lấy được file) cũng khó giải mã nếu khóa được bảo vệ tốt. – **Đáp ứng một phần yêu cầu pháp lý:** Mã hóa giúp thuyết phục rằng dữ liệu khó bị truy cập trái phép, đôi khi cơ quan quản lý chấp thuận (dù không miễn trừ thủ tục,	– **Giới hạn tính năng:** Một số dịch vụ cloud không thể hoạt động trên dữ liệu đã mã hóa (ví dụ search text, hoặc machine learning yêu cầu plaintext). Khách hàng phải chấp nhận hy sinh tính năng hoặc dùng kỹ thuật phức tạp (homomorphic encryption nhưng chưa thực tiễn). – **Quản trị phức tạp:** Quản lý vòng đời khóa, đảm bảo ứng dụng mã hóa/giải mã đúng, tăng độ phức tạp phát triển. – **Rủi ro khóa**: Nếu mất khóa hoặc khóa hỏng, dữ liệu coi như mất (không ai phục hồi). – **Tuân thủ chưa tuyệt đối:** Dù mã hóa, về luật vẫn coi là chuyển dữ liệu. Nếu cơ quan yêu cầu cung cấp dữ liệu dạng rõ phục vụ điều tra, doanh nghiệp vẫn phải giải mã được – tức là có thể phải giao khóa trong trường hợp bất khả kháng.

Tùy chọn kiến trúc	Mô tả	Sử dụng khi	Điều kiện tuân thủ kèm theo	Ưu điểm	Hạn chế & Rủi ro còn lại
				nhưng giảm nguy cơ bị xử lý).	

Tùy chọn kiến trúc	Mô tả	Sử dụng khi	Điều kiện tuân thủ kèm theo	Ưu điểm	Hạn chế & Rủi ro còn lại
6. Multi-Cloud toàn cầu (phân tán theo yêu cầu dịch vụ)	Sử dụng nhiều nhà cung cấp public cloud khác nhau cho các nhu cầu khác nhau, bất kể địa điểm. Ví dụ: dùng AWS ở Singapore cho web, Azure ở Hong Kong cho AI, GCP ở US cho phân tích. Dữ liệu có thể di chuyển giữa các cloud tùy tính năng.	– Doanh nghiệp start-up, công ty công nghệ muốn tận dụng **dịch vụ tốt nhất ở mỗi cloud** (best-of-breed), không quá lo ràng buộc pháp lý địa phương (hoặc có cách đối phó linh hoạt). – Các tổ chức toàn cầu theo kiến trúc microservices, dữ liệu phân mảnh, mỗi phần xử lý ở 1 cloud tối ưu chi phí. – Mức độ chấp nhận rủi ro pháp lý cao, chú trọng hiệu quả kinh doanh.	– Cần **cực kỳ thận trọng phân loại dữ liệu**: cái nào đưa cloud A, cái nào B, để tránh vi phạm (có thể theo quốc gia: dữ liệu EU để cloud EU, dữ liệu VN có thể giữ cloud nào gần VN...). – **DPIA phức tạp:** Phải làm DPIA cho từng luồng chuyển mỗi cloud, hoặc một DPIA bao trùm nhưng nêu rõ nhiều điểm đến. Công tác giấy tờ nhiều. – **Đảm bảo an ninh liên cloud:** Truyền dữ liệu giữa các cloud phải mã hóa và kiểm soát khóa chặt. – **Hợp đồng & giám sát từng bên:** Mỗi CSP phải đánh giá, ký thỏa thuận riêng, theo dõi tuân thủ riêng – rất nặng về quản trị.	– **Tránh phụ thuộc vendor lock-in:** Không bị khóa vào một CSP, giảm rủi ro nếu một bên tăng giá hoặc có sự cố diện rộng (có thể chuyển workload sang cloud khác tạm thời). – **Tối ưu chi phí/tính năng:** Chọn dịch vụ rẻ nhất hoặc tốt nhất cho từng phần (vd cloud A rẻ storage, cloud B AI mạnh). – **Phục vụ thị trường toàn cầu hiệu quả:** Đặt workload gần người dùng mỗi khu vực (theo chiến lược multi-cloud địa lý).	– **Cực kỳ phức tạp vận hành:** Mỗi cloud có hệ thống quản lý, mô hình bảo mật riêng – phải có nhân sự am hiểu tất cả, hoặc xây lớp trừu tượng rất tốn kém. – **Nguy cơ vi phạm chéo:** Dữ liệu có thể "chảy" từ cloud này sang cloud kia ngoài ý muốn (qua nhân viên tải xuống rồi up lên khác) – khó kiểm soát. – **Chồng chéo thủ tục pháp lý:** Nếu dữ liệu cá nhân VN rải nhiều cloud, hồ sơ DPIA phải bao gồm tất cả – dễ sai sót. – **Tấn công bề mặt lớn:** Nhiều môi trường => nhiều điểm yếu có thể bị khai thác nếu không bảo vệ đồng đều. – **Rủi ro pháp lý:** Dữ liệu có thể vô tình chạm đến quốc gia có luật chặt (VD EU GDPR) dẫn đến phải tuân thủ thêm nhiều luật khác song song với luật VN.

Nhìn chung, **phương án 1, 2** dành cho tổ chức ưu tiên tuân thủ, rủi ro rất thấp nhưng đánh đổi chi phí/ công nghệ; **phương án 3, 4** cân bằng trung dung, nhiều tổ chức áp dụng để vừa tuân thủ luật VN vừa hưởng lợi cloud; **phương án 5, 6** nhiều rủi ro tuân thủ hơn, phù hợp tổ chức hiểu biết cao và có chiến lược giảm thiểu riêng. Việc chọn kiến trúc nên dựa trên **phân tích chi phí – lợi ích và khả năng chấp nhận rủi ro** của ban lãnh đạo.

F) Lộ trình triển khai tuân thủ cloud (12–36 tháng)

Việc tuân thủ pháp luật khi chuyển đổi lên cloud không thể làm tức thì, cần lộ trình nhiều giai đoạn. Dưới đây là đề xuất **roadmap 12–36 tháng** với các giai đoạn, kết quả chính, chỉ số (KPI) để đo lường, rủi ro trong mỗi giai đoạn và kiểm soát tương ứng:

Bảng: Roadmap triển khai tuân thủ Cloud

Giai đoạn	Kết quả cần đạt (Deliverables)	KPI đo lường	Rủi ro trong giai đoạn	Biện pháp kiểm soát/ giảm thiểu
0–6 tháng: Chuẩn bị & Đánh giá hiện trạng (Phase 1)	– **Thành lập nhóm dự án Cloud Compliance** gồm pháp chế, ATTT, CNTT, các bên liên quan. – **Đào tạo ban đầu**: phổ biến cho lãnh đạo và nhóm dự án về yêu cầu pháp lý cloud (có thể sử dụng tài liệu này). – **Đánh giá hiện trạng dữ liệu & hệ thống:** lập **data inventory** và phân loại (Deliverable: Bảng phân loại dữ liệu theo yêu cầu pháp lý – từ phần C). – **Đánh giá nhà cung cấp cloud tiềm năng:** shortlist các CSP đáp ứng tiêu chí (Deliverable: Báo cáo đánh giá NCC, so sánh tuân thủ). – **Kế hoạch chuyển đổi chi tiết:** xây dựng kế hoạch chuyển từng phần hệ thống nào lên cloud, chọn kiến trúc (Deliverable: Tài liệu Kiến trúc Cloud tuân thủ đã duyệt).	– **100% nhóm dự án được đào tạo** căn bản trong 2 tháng đầu (KPI: hoàn thành khóa train, quiz >80 điểm). – **Danh mục dữ liệu hoàn thành** trước tháng thứ 3 (KPI: có inventory phê duyệt). – **Báo cáo đánh giá CSP hoàn thành** trước tháng 4 (KPI: ít nhất 2 CSP được đánh giá tuân thủ, có điểm số). – **Kiến trúc & kế hoạch được phê duyệt** bởi lãnh đạo trước tháng 6.	– **Thiếu nhận thức & ủng hộ:** nếu lãnh đạo/ phòng ban chưa hiểu nhu cầu tuân thủ, dự án có thể bị xem nhẹ. – **Dữ liệu phân tán, khó thu thập:** inventory ban đầu mất thời gian, có thể sót dữ liệu, ảnh hưởng thiết kế. – **Chọn sai CSP:** đánh giá không kỹ có thể chọn nhà cung cấp không phù hợp, về sau gặp vấn đề tuân thủ.	– Tổ chức **hội thảo lãnh đạo**: mời chuyên gia (hoặc sử dụng tài liệu) để thuyết phục tầm quan trọng, kiếm **người đỡ đầu** (sponsor) cấp cao. – Sử dụng **bảng câu hỏi chi tiết** cho các phòng ban để thu thập thông tin dữ liệu; có văn bản yêu cầu và hạn chót để họ cung cấp. Kiểm tra chéo với hệ thống hiện tại (VD: quét CSDL, share nội bộ) để không sót. – Tham vấn **đơn vị tư vấn độc lập** hỗ trợ đánh giá CSP về tuân thủ (nếu nội bộ chưa đủ kinh nghiệm), giảm nguy cơ chủ quan.

Giai đoạn	Kết quả cần đạt (Deliverables)	KPI đo lường	Rủi ro trong giai đoạn	Biện pháp kiểm soát/ giảm thiểu
6–18 tháng: Xây dựng chính sách & Triển khai thí điểm (Phase 2)	– **Xây dựng bộ chính sách & quy trình:** hoàn thiện các **policy** về phân loại dữ liệu, chính sách an ninh cloud, quy trình DPIA, quy trình quản lý sự cố cloud… (Deliverable: Bộ Chính sách Cloud Compliance ban hành). – **Ký hợp đồng với CSP đã chọn:** hoàn tất đàm phán hợp đồng, DPA (Deliverable: Hợp đồng chứa các điều khoản đạt yêu cầu checklist D). – **Thực hiện DPIA cho dự án thí điểm:** chuẩn bị Hồ sơ DPIA và gửi Bộ CA (Deliverable: Hồ sơ đã gửi, có biên nhận). – **Triển khai thí điểm 1–2 ứng dụng lên cloud:** ưu tiên ứng dụng không quá nhạy cảm nhưng có giá trị (Deliverable: Ứng dụng chạy trên cloud trong môi trường thật, có giám sát). – **Kiểm tra, rút kinh nghiệm từ thí điểm:** đánh giá xem chính sách, quy trình có hoạt động hiệu quả không (Deliverable: Báo cáo đánh giá thí điểm, kiến nghị cải thiện).	– **100% chính sách, quy trình liên quan được ban hành** trong 9 tháng đầu (KPI: có số hiệu văn bản, lãnh đạo ký duyệt). – **Hợp đồng cloud ký kết** trước tháng 12 (KPI: hoàn thành pháp lý, không điều khoản nào vi phạm checklist). – **DPIA nộp Bộ CA** xong trước khi go-live thí điểm (KPI: nộp đúng hạn, không bị yêu cầu bổ sung quá 1 lần). – **Ứng dụng thí điểm chạy ổn định** trong 3 tháng liên tục (KPI: Uptime >99%, không sự cố bảo mật nghiêm trọng). – **Báo cáo sau thí điểm** hoàn thành tháng 18 với các bài học.	– **Chính sách trên giấy, khó áp dụng:** nhân viên có thể chưa quen quy trình DPIA, phân loại, dẫn đến thực hiện không đúng (ví dụ dự án quên làm DPIA). – **Đàm phán hợp đồng kéo dài:** CSP lớn có thể chậm phản hồi pháp lý, khiến dự án chậm. – **Vấn đề kỹ thuật trong thí điểm:** có thể xảy ra sự cố hoặc hiểu sai cấu hình an toàn, gây mất niềm tin. – **Cơ quan NN phản hồi chậm DPIA:** nếu hồ sơ bị treo lâu, dự án có thể trì trệ.	– Triển khai **chương trình truyền thông nội bộ** song song: ví dụ phát hành cẩm nang ngắn “Quy trình mới khi dùng cloud” tới quản lý dự án, tích hợp vào checklist phê duyệt dự án CNTT để không ai quên. – **Escalate sớm**: nếu hợp đồng bế tắc điều khoản nào, báo cáo lãnh đạo để họ có thể chấp thuận mức độ rủi ro hoặc đưa quan hệ cao hơn làm việc với CSP. – Với thí điểm: bắt đầu từ **môi trường non-prod** (dev/test) trước, kiểm thử an toàn (pentest) rồi mới chuyển prod, giảm rủi ro. – Chủ động **theo dõi hồ sơ DPIA**: liên hệ thường xuyên Cục A05 hỏi tiến độ, bổ sung ngay nếu cần, tránh để lâu.

Giai đoạn	Kết quả cần đạt (Deliverables)	KPI đo lường	Rủi ro trong giai đoạn	Biện pháp kiểm soát/ giảm thiểu
18–30 tháng: Mở rộng quy mô & Chứng nhận (Phase 3)	– **Mở rộng triển khai cloud cho các hệ thống khác:** dựa trên kinh nghiệm thí điểm, đưa thêm các workload phù hợp lên cloud (Deliverable: Danh sách hệ thống migrat lên cloud giai đoạn 2, kèm DPIA nếu có). – **Tích hợp đầy đủ với quy trình CNTT & ATTT:** mọi dự án mới đều thực hiện phân loại dữ liệu, DPIA nếu cần, đánh giá bảo mật cloud trước go-live (Deliverable: Update quy trình phát triển và triển khai phần mềm có bước check cloud compliance). – **Đạt được chứng nhận tuân thủ (nếu định hướng):** ví dụ đạt chứng chỉ **ISO 27001** cho hệ thống thông tin bao gồm môi trường cloud, hoặc chứng nhận **Level 3/4 đảm bảo ATTT** từ Bộ TT&TT (Deliverable: Giấy chứng nhận, báo cáo audit). – **Kiểm toán nội bộ lần 1:** tiến hành audit độc lập nội bộ sau ~1 năm vận hành (Deliverable: Báo cáo kiểm toán nội bộ cloud compliance). – **Điều chỉnh chính sách, hợp đồng nếu luật thay đổi:** ví dụ Luật Bảo vệ DL cá nhân ban hành thay NĐ13 (giả định) – cập nhật kịp thời (Deliverable: Chính sách sửa đổi, phụ lục hợp đồng bổ sung mới).	– **Số hệ thống triển khai cloud tăng** ít nhất 50% so với thí điểm (KPI: ví dụ từ 2 ứng dụng lên 5 ứng dụng). – **Không có vi phạm pháp luật nào xảy ra** trong quá trình mở rộng (KPI: 0 lần bị cơ quan nhắc nhở hay xử phạt). – **Chứng chỉ đạt được** (nếu đặt mục tiêu): KPI: đạt ISO 27001 trước tháng 24, hoặc chứng nhận mức 3 ATTT từ Bộ. – **Audit nội bộ:** phát hiện < 5 điểm không phù hợp nhỏ, không có điểm lớn (KPI). – **Chính sách luôn cập nhật:** mọi văn bản chính sách không quá 3 tháng kể từ khi luật mới hiệu lực (KPI: thời gian cập nhật luật).	– **Quá tải quản lý khi mở rộng:** nhiều hệ thống lên cloud -> nhiều dự án DPIA, đánh giá bảo mật – có nguy cơ thiếu nhân lực làm kỹ các thủ tục, dẫn đến làm qua loa. – **Nguy cơ sự cố khi scale:** khi nhiều team dùng cloud, khả năng ai đó cấu hình sai gây lộ thông tin tăng. – **Chứng nhận tốn kém thời gian:** chuẩn bị ISO có thể kéo dài, làm ảnh hưởng công việc khác. – **Luật mới bất ngờ:** ví dụ nếu Luật An ninh mạng có nghị định mới thu hẹp phạm vi dùng cloud nước ngoài, phải thay đổi kế hoạch.	– **Tự động hóa & training:** đầu tư công cụ CSPM để giám sát cấu hình tự động, giảm tải cho đội tuân thủ. Đào tạo thêm thành viên các đội (DevOps, Sysadmin) để họ tự làm đúng phần mình (shift-left compliance). – **Mở rộng từ từ theo ưu tiên:** không dàn trải tất cả cùng lúc. Xác định hệ thống ưu tiên (theo lợi ích kinh doanh và rủi ro chấp nhận được). Giữ một số hệ thống on-prem lâu hơn nếu cần thêm kiểm chứng. – **Đặt nhóm phụ trách chứng nhận riêng** (nếu có thể thuê tư vấn ISO) để nhóm vận hành tập trung vận hành, tránh quá tải. – Theo dõi sát thông tin dự thảo luật, tham gia góp ý nếu có cơ hội (qua hiệp hội ngành) để lường trước thay đổi. Kịp thời cập nhật lãnh đạo và chính sách nội bộ.

Giai đoạn	Kết quả cần đạt (Deliverables)	KPI đo lường	Rủi ro trong giai đoạn	Biện pháp kiểm soát/ giảm thiểu
30–36 tháng: Hoàn thiện & Duy trì (Phase 4)	– **Chính thức vận hành "Cloud Compliance" BAU:** tích hợp hoàn toàn vào chu trình CNTT: check tuân thủ là bước bắt buộc trước phê duyệt kiến trúc, trước go-live. (Deliverable: Mô tả quy trình vận hành chuẩn). – **Bàn giao trách nhiệm từ dự án sang thường xuyên:** chuyển từ chế độ dự án sang giao cho bộ phận thường trực (ví dụ DPO/ Data Governance team) quản lý dài hạn. (Deliverable: Quyết định phân công đơn vị chủ trì quản lý tuân thủ cloud). – **Giám sát liên tục & cải tiến:** có dashboard KPI định kỳ (hàng quý) về tình hình tuân thủ (số DPIA đã làm, sự cố, tập huấn...) báo cáo lãnh đạo. (Deliverable: Báo cáo quý gửi Ban giám đốc). – **Đánh giá bên ngoài (nếu cần):** mời kiểm toán độc lập đánh giá việc tuân thủ hoặc khi chuẩn bị cho thanh tra. (Deliverable: Báo cáo đánh giá độc lập). – **Đáp ứng thanh tra (nếu xảy ra):** chuẩn bị hồ sơ và trả lời cơ quan nếu có thanh tra định kỳ. (Deliverable: Hồ sơ làm việc với đoàn thanh tra, biên bản).	– **Tuân thủ trở thành hoạt động thường xuyên:** không còn ở dạng "dự án", KPI: 100% dự án mới đã áp dụng quy trình, 0 trường hợp "đi tắt" bỏ qua DPIA. – **Báo cáo quản trị được thực hiện đúng hạn** (KPI: 4/4 quý có báo cáo). – **Không có sự cố tuân thủ nghiêm trọng:** (KPI: 0 lần bị phạt; 0 khiếu nại người dùng về dữ liệu cá nhân). – **Chuẩn bị cho thanh tra:** (KPI: khi thanh tra, không bị kết luận vi phạm nào).	– **Nguy cơ chủ quan dần:** Sau 2-3 năm không sự cố lớn, có thể xuất hiện tâm lý chủ quan, cắt giảm nguồn lực tuân thủ. – **Thay đổi nhân sự:** Dự án có thể mất người giỏi (nhảy việc), kiến thức tuân thủ bị mai một. – **Môi trường thay đổi:** CSP thay đổi chính sách, xuất hiện dịch vụ cloud mới nhân viên tự dùng (shadow IT) gây mất kiểm soát. – **Thanh tra đột xuất:** nếu xảy ra vi phạm trong ngành, cơ quan có thể kiểm tra gắt gao – doanh nghiệp cần sẵn sàng.	– **Thiết lập văn hóa tuân thủ:** đưa nội dung tuân thủ cloud vào KPI công việc của các phòng ban (VD: phòng phát triển phải bảo đảm DPIA cho sản phẩm mới). Khen thưởng các nhóm làm tốt, phê bình nếu vi phạm quy trình. – **Xây dựng đội ngũ kế cận:** luân chuyển nhân viên qua lại giữa nhóm dự án và vận hành thường trực để truyền kiến thức. Tài liệu hóa quy trình, bài học đầy đủ để người mới tiếp quản được. – **Cập nhật liên tục:** DPO/Compliance cần duy trì kết nối cộng đồng (VNISA, IAPP) để cập nhật xu hướng, sớm phát hiện nguy cơ (ví dụ ChatGPT gây rò dữ liệu? nhân viên dùng, phải đưa vào chính sách mới). – **Drill thanh tra nội bộ:** thỉnh thoảng giả lập tình huống thanh tra đến trong 1 tuần – đội tự rà soát hồ sơ, giúp luôn sẵn sàng và tự phát hiện lỗ hổng giấy tờ để bổ sung trước.

Như vậy, lộ trình 3 năm sẽ giúp tổ chức **từng bước chuyển đổi lên public cloud một cách tuân thủ**, giảm thiểu các cú sốc và rủi ro pháp lý. Quan trọng là duy trì **cam kết từ lãnh đạo**, **đào tạo nhân sự liên tục** và **cải tiến không ngừng** dựa trên kinh nghiệm triển khai thực tế. Với khung tuân thủ và kiểm soát đã đề ra,

doanh nghiệp có thể tự tin hưởng lợi từ công nghệ cloud mà vẫn đảm bảo đáp ứng các yêu cầu pháp luật Việt Nam hiện hành.

---

1 2 3 4 5 Luật An ninh mạng 2018, số 24/2018/QH14
https://luatvietnam.vn/an-ninh-quoc-gia/luat-an-ninh-mang-2018-so-24-2018-qh14-164904-d1.html

6 7 8 9 10 11 Vietnam: Cybersecurity Data Localization Requirements
https://www.trade.gov/market-intelligence/vietnam-cybersecurity-data-localization-requirements

12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 66 67 68 69 71 75 76 77 80 Nghị định 13/2023/NĐ-CP bảo vệ dữ liệu cá nhân
https://xaydungchinhsach.chinhphu.vn/toan-van-nghi-dinh-13-2023-nd-cp-bao-ve-du-lieu-ca-nhan-119230516104357809.htm

44 47 48 49 50 51 52 53 Nghị định 85/2016/NĐ-CP bảo đảm an toàn hệ thống thông tin theo cấp độ mới nhất
https://thuvienphapluat.vn/van-ban/Cong-nghe-thong-tin/Nghi-dinh-85-2016-ND-CP-bao-dam-an-toan-he-thong-thong-tin-theo-cap-do-317475.aspx

45 5 cấp độ bảo đảm an toàn hệ thống thông tin theo Nghị định 85 ...
https://sunteco.vn/5-cap-do-bao-dam-an-toan-he-thong-thong-tin/

46 5 cấp độ bảo đảm an toàn hệ thống thông tin trên môi trường mạng
https://diemthuy.thainguyen.gov.vn/cam-nang-an-toan-thong-tin/5-cap-do-bao-dam-an-toan-he-thong-thong-tin-tren-moi-truong-mang-47310

54 Luật Bảo vệ bí mật Nhà nước mới nhất, số 29/2018/QH14
https://luatvietnam.vn/an-ninh-quoc-gia/luat-bao-ve-bi-mat-nha-nuoc-2018-169341-d1.html

55 Luật Bảo vệ bí mật nhà nước số 29/2018/QH14 ngày 15/11/2018 ...
https://tulieuvankien.dangcongsan.vn/he-thong-van-ban/van-ban-quy-pham-phap-luat/luat-bao-ve-bi-mat-nha-nuoc-so-292018qh14-ngay-15112018-hieu-luc-thi-hanh-tu-ngay-0172020-5070

56 Tổng hợp các văn bản hướng dẫn Luật Bảo vệ bí mật nhà nước mới ...
https://www.vinacas.com.vn/tong-hop-cac-van-ban-huong-dan-luat-bao-ve-bi-mat-nha-nuoc-moi-nhat-nam-2025-bv4021.htm

57 Dự thảo Nghị định quy định chi tiết và biện pháp thi hành Luật Bảo ...
https://bocongan.gov.vn/chinh-sach-phap-luat/bai-viet/du-thao-nghi-dinh-quy-dinh-chi-tiet-va-bien-phap-thi-hanh-luat-bao-ve-bi-mat-nha-nuoc-sua-doi-1755512103

58 Luật số 29/2018/QH14 của Quốc hội: Luật Bảo vệ bí mật nhà nước
https://vanban.chinhphu.vn/?pageid=27160&docid=206098

59 Luật bảo vệ bí mật nhà nước - Sở Khoa học và Công nghệ TPHCM
https://dost.hochiminhcity.gov.vn/van-ban-quy-pham-phap-luat/luat-bao-ve-bi-mat-nha-nuoc/

60 CMC Cloud - Cổng thông tin Nghị quyết 57
https://nq57.mst.gov.vn/products/330

61 62 63 64 65 74 Ngân hàng đảm bảo an toàn thông tin điện toán đám mây
https://vietnamnet.vn/ngan-hang-dam-bao-an-toan-thong-tin-dien-toan-dam-may-2241564.html

70 Từ 1/10, dữ liệu thông tin cá nhân người dùng tại Việt Nam phải ...
https://vneconomy.vn/tu-1-10-du-lieu-thong-tin-ca-nhan-nguoi-dung-tai-viet-nam-phai-duoc-luu-tru-trong-nuoc.htm

72 73 78 79 81 Quyền và nghĩa vụ của doanh nghiệp cung cấp dịch vụ trung tâm dữ liệu, dịch vụ điện toán đám mây được quy định như thế nào?

https://thuvienphapluat.vn/phap-luat/ho-tro-phap-luat/quyen-va-nghia-vu-cua-doanh-nghiep-cung-cap-dich-vu-trung-tam-du-lieu-dich-vu-dien-toan-dam-may-duo-734742-153472.html