CDLAF
YOUR CONFIDANT

/2026

SỬ DỤNG CÁC DỊCH VỤ ĐIỆN TOÁN ĐÁM MÂY NƯỚC NGOÀI VÀ CHUYỂN DỮ LIỆU CÁ NHÂN XUYÊN BIÊN GIỚI: DOANH NGHIỆP CẦN LƯU Ý GÌ?

PHẦN 2: DOANH NGHIỆP CẦN LÀM GÌ KHI CÓ HOẠT ĐỘNG CHUYỂN DỮ LIỆU CÁ NHÂN XUYÊN BIÊN GIỚI?

Tác giả:

Hà Lữ Chí Đạt
Luật sư Cấp cao

Phạm Thị Hoài
Chuyên viên pháp lý Cấp cao

PHẦN 2: DOANH NGHIỆP CẦN LÀM GÌ KHI CÓ HOẠT ĐỘNG CHUYỂN DỮ LIỆU CÁ NHÂN XUYÊN BIÊN GIỚI?

Tại **Phần 1**, chúng ta đã làm rõ các tiêu chí kỹ thuật và pháp lý để nhận diện khi nào việc sử dụng dịch vụ điện toán đám mây từ nhà cung cấp dịch vụ nước ngoài (AWS, Azure, Google Cloud...) dẫn đến phát sinh nghĩa vụ thực hiện thủ tục về báo cáo tác động chuyển dữ liệu cá nhân xuyên biên giới, các trường hợp ngoại lệ theo quy định. Vậy khi đã xác định được chính xác nghĩa vụ phải thực hiện thì về phía doanh nghiệp sẽ cần chuẩn bị những nội dung nào thuộc về nhân sự, kỹ thuật, văn bản quản lý nội bộ để đáp ứng được yêu cầu của cơ quan quản lý? Trường hợp doanh nghiệp chậm trễ thực hiện thì có phát sinh các khoản phạt cho doanh nghiệp không, tất cả những vấn đề này sẽ được CDLAF chia sẻ tại Phần 2 dưới đây.

1. Doanh nghiệp cần làm gì khi có hoạt động chuyển dữ liệu cá nhân xuyên biên giới?

Về tổng quan, pháp luật yêu cầu cơ quan, tổ chức, cá nhân có hoạt động chuyển dữ liệu cá nhân xuyên biên giới phải lập báo cáo đánh giá tác động trong vòng 60 ngày kể từ ngày bắt đầu. Theo đây, sau khi doanh nghiệp xác định có hoạt động chuyển dữ liệu cá nhân xuyên biên giới có thể tham khảo các bước cơ bản sau:

Bước 1: Thiết lập bản đồ luồng dữ liệu (Data Flow Mapping) và xác định tư cách pháp lý của các bên trong hoạt động xử lý dữ liệu

Đây là bước nền tảng quyết định tính chuẩn xác của toàn bộ hồ sơ. Nếu xác định sai luồng dữ liệu hoặc nhầm lẫn vai trò pháp lý ngay từ đầu, doanh nghiệp sẽ phải điều chỉnh lại toàn bộ hệ thống đánh giá rủi ro và các cam kết trong hợp đồng. Doanh nghiệp cần triển khai bóc tách 3 nội dung cơ bản sau:

- Khoanh vùng và Thiết lập Bản đồ đường đi của dữ liệu: Theo đó, doanh nghiệp sẽ cần xác định chi tiết từng loại dữ liệu cá nhân sẽ có khả năng dịch chuyển xuyên biên giới, có bao gồm các dữ liệu cá nhân nhạy cảm hay không, điểm xuất phát của dữ liệu, và dữ liệu sẽ được dịch chuyển xuyên biên giới thông qua các công cụ vật lý hay các nền tảng, phần mềm nào, vị trí địa lý của máy chủ tiếp nhận, xử lý dữ liệu cá nhân...
- Mục đích dữ liệu cá nhân được chuyển dữ liệu xuyên biên giới là gì?: Điều này để xác định dữ liệu cá nhân được dịch chuyển xuyên biên giới có thuộc trường hợp phải thực hiện thủ tục hay không, theo đó sẽ cần xác định mục đích công ty ở Việt Nam chuyển dữ liệu cá nhân xuyên biên giới là cho nhu cầu cung cấp thông tin cho công ty mẹ, hay cung cấp cho đối tác để thực hiện các mục đích khác liên quan đến hoạt động kinh doanh, cho mục đích lưu trữ như sao lưu an toàn trên hạ tầng điện toán đám mây, hay vận hành hệ thống ERP quốc tế...

PHẦN 2: DOANH NGHIỆP CẦN LÀM GÌ KHI CÓ HOẠT ĐỘNG CHUYỂN DỮ LIỆU CÁ NHÂN XUYÊN BIÊN GIỚI?

- Xác lập chính xác Tư cách Pháp lý của các bên liên quan: Theo đó, doanh nghiệp sẽ cần xác định và đối chiếu với quy định của pháp luật bảo vệ dữ liệu cá nhân thì bên Việt Nam là bên kiểm soát dữ liệu cá nhân, Bên xử lý dữ liệu cá nhân hay là bên vừa kiểm soát và xử lý dữ liệu cá nhân. Đồng thời bên nước ngoài – bên tiếp nhận dữ liệu cá nhân từ doanh nghiệp tại Việt Nam là bên thứ 3 độc lập, công ty mẹ con trong cùng tập đoàn và vai trò của bên nước ngoài theo pháp luật dữ liệu cá nhân là gì.

Bước 2: Chuẩn bị hồ sơ đánh giá tác động

Doanh nghiệp cần chuẩn bị hồ sơ đánh giá tác động xử lý dữ liệu cá nhân xuyên biên giới theo quy định. Một nội dung cần được chuẩn bị sớm là thông tin về người hoặc bộ phận phụ trách bảo vệ dữ liệu cá nhân. Người hoặc bộ phận này có thể do doanh nghiệp bố trí nội bộ hoặc thuê tổ chức, cá nhân cung cấp dịch vụ phù hợp. Doanh nghiệp cũng cần lưu ý yêu cầu liên quan đến việc nhân sự phụ trách được đào tạo, bồi dưỡng kiến thức về bảo vệ dữ liệu cá nhân. Trong giai đoạn này, doanh nghiệp cần tập trung vào 2 cấu phần cốt lõi:

Quyết định lựa chọn Nhân sự / Bộ phận Bảo vệ dữ liệu cá nhân (DPO Setup): Theo đó doanh nghiệp có thể lựa chọn một trong hai phương án:

- **Mô hình Nhân sự nội bộ (In-house DPO):** Ban hành Quyết định bổ nhiệm chính thức từ Người đại diện theo pháp luật. Nhân sự này bắt buộc phải hoàn thành chương trình đào tạo, bồi dưỡng kiến thức về bảo vệ dữ liệu cá nhân theo quy định.
- **Mô hình Thuê ngoài (DPO-as-a-Service):** Ký kết hợp đồng dịch vụ với tổ chức, công ty luật hoặc đơn vị chuyên môn. Phương án này tối ưu chi phí vận hành cho doanh nghiệp và đảm bảo tính khách quan, độc lập khi giám sát tuân thủ.

Chuẩn hóa các nội dung kỹ thuật trong Hồ sơ Đánh giá tác động:

- **Xác định tư cách pháp lý và thông tin các bên:** Định danh đầy đủ thông tin pháp nhân của Bên chuyển giao tại Việt Nam (Data Exporter) và Bên tiếp nhận tại nước ngoài (Data Importer - công ty mẹ, nhà cung cấp SaaS/Cloud quốc tế).
- **Mô tả mục đích, luồng đi của dữ liệu:** Giải trình rõ ràng vì sao hoạt động xử lý dữ liệu bắt buộc phải thực hiện trên máy chủ đặt ngoài lãnh thổ Việt Nam mà không thể xử lý hoàn toàn trong nước.

- **Bản thuyết minh biện pháp kỹ thuật và an toàn thông tin:** Mô tả chi tiết các giải pháp kỹ thuật bảo vệ dữ liệu: chuẩn mã hóa khi truyền đưa và lưu trữ, cơ chế quản lý khóa mã hóa, chính sách phân quyền truy cập tối thiểu, quy trình ghi nhận nhật ký (System Logs).

Có thể thách thức hiện tại của đa số các doanh nghiệp là vấn đề về chi phí tài chính để tuân thủ, bởi khi thực hiện các quy định mà pháp luật bảo vệ dữ liệu cá nhân đặt ra thì chi phí đầu tiên phải kể đến là chi phí nhân sự DPO. Doanh nghiệp sẽ không đơn thuần để một nhân sự bất kỳ kiêm nhiệm với một quyết định nội bộ của công ty, mà nhân sự đó sẽ phải đã trải qua khóa đào tạo chuyên môn về DPO. Mặc dù vậy ngay cả khi công ty sắp xếp cho nhân sự tham gia các khóa đào tạo thì việc để nhân sự đó chấp nhận kiêm nhiệm thêm vai trò DPO thực sự không dễ dàng, điều này xuất phát từ tính trách nhiệm của vị trí này khá lớn, đặc biệt là khi xảy ra các sự cố rò rỉ dữ liệu, hoặc ở một mức độ nào đó công ty có vi phạm về tuân thủ DLCN thì ít nhiều sẽ có phát sinh trách nhiệm của DPO.

Bước 3: Hoàn thiện các tài liệu và chính sách liên quan

Hồ sơ Đánh giá tác động chỉ là văn bản mang tính thủ tục hành chính để nộp lên A05, đi kèm theo báo cáo, doanh nghiệp sẽ phải đảm bảo doanh nghiệp đã có đầy đủ các chính sách, quy trình mà pháp luật yêu cầu phải có cho mục đích doanh nghiệp có đầy đủ tư cách để xử lý dữ liệu cá nhân, theo đó về cơ bản sẽ có các văn bản quan trọng sau:

- **Chính sách bảo vệ dữ liệu cá nhân:** Chính sách được thể hiện bằng quy chế nội bộ của công ty, quy chế sẽ phân định quyền truy cập dữ liệu, tiêu chuẩn bảo mật thiết bị đầu cuối và trách nhiệm bảo mật của nhân sự nội bộ ... Đối với các văn bản được xác lập giữa doanh nghiệp với các bên thứ ba như người lao động, khách hàng, đối tác ... thì cần thiết phải có thêm các điều khoản hoặc phụ lục hợp đồng để ghi nhận cam kết thỏa thuận của công ty về xử lý dữ liệu cá nhân có liên quan. Lưu ý rằng, trường hợp doanh nghiệp có thêm các nền tảng thương mại điện tử thì sẽ cần xây dựng lại các nội dung về Điều khoản sử dụng, Chính sách quyền riêng tư, điều khoản về sự đồng ý của người dùng...
- **Sơ đồ luồng dữ liệu:** Số hóa bản đồ đường đi của dữ liệu: từ điểm thu thập đầu vào tại Việt Nam, giao thức truyền đưa an toàn (API, mã hóa đường truyền TLS), đến vị trí địa lý của hệ thống máy chủ lưu trữ chính (Primary Server) ...Xác lập danh mục các trường thông tin cụ thể (dữ liệu cơ bản hay dữ liệu nhạy cảm) tương ứng với từng điểm tiếp nhận dữ liệu ở nước ngoài.

- **Hệ thống biểu mẫu và quy trình vận hành chuẩn:** Bộ biểu mẫu tiếp nhận và xử lý yêu cầu của chủ thể dữ liệu (rút lại sự đồng ý, yêu cầu xóa, hạn chế hoặc cung cấp bản sao dữ liệu). Quy trình ứng phó và xử lý sự cố an ninh dữ liệu khẩn cấp (Incident Response Plan), phân định rõ vai trò của DPO, bộ phận IT/Security và Ban Điều hành khi xảy ra rủi ro lộ lọt dữ liệu.

Bước 4: Nộp hồ sơ đến cơ quan có thẩm quyền

Sau khi hoàn thiện hồ sơ, doanh nghiệp thực hiện việc nộp hồ sơ, theo đó doanh nghiệp gửi 01 bộ hồ sơ chính thức đến Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao (A05 - Bộ Công an) trong thời hạn 60 ngày kể từ ngày bắt đầu phát sinh hoạt động chuyển dữ liệu. Bản gốc của toàn bộ hồ sơ đánh giá tác động, tài liệu chứng minh và DPA phải luôn sẵn sàng lưu trữ tại trụ sở doanh nghiệp để phục vụ công tác thanh tra, hậu kiểm.

Bước 5: Theo dõi kết quả xử lý, phối hợp giải trình và duy trì trạng thái tuân thủ hậu kiểm

Sau khi nộp hồ sơ, nghĩa vụ của doanh nghiệp không dừng lại ở việc nhận biên nhận mà chuyển sang giai đoạn phối hợp thẩm định và quản trị rủi ro vận hành thực tế: Chủ động theo dõi tình trạng xử lý hồ sơ, chuẩn bị sẵn sàng nhân sự chuyên trách khi nhận được yêu cầu làm rõ.

Thiết lập và lưu trữ Hồ sơ tại trụ sở doanh nghiệp: Doanh nghiệp bắt buộc phải lưu giữ 01 bộ hồ sơ gốc (văn bản giấy và dữ liệu điện tử) tại trụ sở chính, bao gồm: Hồ sơ đánh giá tác động chính thức, bản sao DPA, bằng chứng chấp thuận của người dùng và các chính sách bảo mật nội bộ. Cơ quan có thẩm quyền có thể tiến hành kiểm tra đột xuất hoặc định kỳ. Hồ sơ lưu trữ tại doanh nghiệp phải luôn phản ánh đúng thực tế hạ tầng và luồng dữ liệu đang vận hành.

Doanh nghiệp cần lưu ý rằng, doanh nghiệp sẽ buộc phải cập nhật hồ sơ định kỳ khi có thay đổi như: Thay đổi hoặc bổ sung nhà cung cấp Cloud/SaaS; Thay đổi cấu hình hạ tầng máy chủ hoặc vị trí địa lý của trung tâm dữ liệu; Mở rộng phạm vi thu thập hoặc chuyển giao thêm các trường dữ liệu cá nhân nhạy cảm mới (dữ liệu thanh toán, sinh trắc học, hồ sơ sức khỏe); Tái cấu trúc doanh nghiệp, sáp nhập hoặc thay đổi đơn vị tiếp nhận dữ liệu tại tập

đoàn mẹ ở nước ngoài...

2. Những trường hợp nào không phải thực hiện đánh giá tác động chuyển dữ liệu cá nhân xuyên biên giới?

Không phải mọi hoạt động chuyển dữ liệu cá nhân xuyên biên giới đều phải thực hiện hồ sơ đánh giá tác động. Theo khoản 6 Điều 20 Luật Bảo vệ dữ liệu cá nhân 2025 và khoản 3 Điều 17 Nghị định 356/2025/NĐ-CP, một số trường hợp không phải thực hiện quy định về đánh giá tác động chuyển dữ liệu cá nhân xuyên biên giới, bao gồm:

- Chuyển dữ liệu cá nhân xuyên biên giới của cơ quan nhà nước có thẩm quyền;
- Cơ quan, tổ chức lưu trữ dữ liệu cá nhân của người lao động thuộc cơ quan, tổ chức đó trên dịch vụ điện toán đám mây;
- Chủ thể dữ liệu cá nhân tự chuyển dữ liệu cá nhân của mình xuyên biên giới;
- Hoạt động báo chí, truyền thông theo quy định của pháp luật;
- Việc chuyển dữ liệu cá nhân xuyên biên giới đã được công khai theo quy định của pháp luật;
- Trường hợp khẩn cấp, thực sự cần thiết phải cung cấp dữ liệu cá nhân xuyên biên giới để bảo vệ tính mạng, sức khỏe, an toàn tài sản của cá nhân hoặc để thực hiện nhiệm vụ, nghĩa vụ theo quy định pháp luật;
- Chuyển dữ liệu cá nhân xuyên biên giới để quản lý nhân sự xuyên biên giới theo quy tắc, quy chế lao động và thỏa ước lao động tập thể theo quy định pháp luật;
- Cung cấp dữ liệu cá nhân xuyên biên giới để ký kết hợp đồng hoặc thực hiện các thủ tục liên quan đến vận chuyển xuyên biên giới, hậu cần, chuyển tiền, thanh toán, khách sạn, xin thị thực, xin học bổng.

Do đó, khi xác định nghĩa vụ của doanh nghiệp, cần kiểm tra cả trường hợp chuyển dữ liệu và các trường hợp được loại trừ, thay vì mặc nhiên cho rằng cứ có dữ liệu được chuyển ra nước ngoài là phải lập hồ sơ đánh giá tác động.

Tuy nhiên, doanh nghiệp cũng cần lưu ý rằng việc không phải đánh giá tác động trên không đồng nghĩa với việc doanh nghiệp được miễn nghĩa vụ tuân thủ với các quy định khác về bảo vệ và xử lý dữ liệu cá nhân, bao gồm cả các công việc như thiết lập bản đồ luồng dữ liệu, xác định tư cách pháp lý

của các bên trong hoạt động xử lý dữ liệu, hoàn thiện các chính sách có liên quan, v.v...

3. Rủi ro pháp lý và Tổn thất kinh doanh nếu không nộp hồ sơ đúng hạn

Vừa qua vào ngày 19 tháng 8 năm 2026, Chính phủ cũng đã ban hành Nghị định số 330/2026/NĐ-CP quy định xử phạt vi phạm hành chính trong lĩnh vực an ninh mạng và bảo vệ dữ liệu cá nhân và có hiệu lực vào cùng ngày.

Như một hệ quả, việc doanh nghiệp thực hiện hồ sơ báo cáo tác động chuyển dữ liệu xuyên biên giới sẽ không còn là câu chuyện "lựa chọn" hay tạm thời chưa thực hiện hay chưa cấp thiết.

Theo nghị định mới ban hành mức xử phạt tùy theo hành vi có thể là một số tiền cụ thể và cũng có thể được xác định theo một tỉ lệ phạt dựa trên doanh thu, cụ thể:

Mức phạt tiền	Hành vi
30.000.000 đồng đến **50.000.000 đồng**	• Không lập hồ sơ đánh giá tác động chuyển dữ liệu cá nhân xuyên biên giới trước hoặc trong thời gian tiến hành chuyển dữ liệu; • Không cập nhật định kỳ hoặc không cập nhật hồ sơ đánh giá tác động chuyển dữ liệu cá nhân xuyên biên giới khi có thay đổi theo quy định pháp luật; • Không duy trì hồ sơ đánh giá tác động chuyển dữ liệu cá nhân xuyên biên giới ở trạng thái sẵn sàng phục vụ hoạt động kiểm tra của cơ quan chuyên trách bảo vệ dữ liệu cá nhân ...

PHẦN 2: DOANH NGHIỆP CẦN LÀM GÌ KHI CÓ HOẠT ĐỘNG CHUYỂN DỮ LIỆU CÁ NHÂN XUYÊN BIÊN GIỚI?

Mức phạt tiền	Hành vi
50.000.000 đồng đến **100.000.000 đồng**	• Không xác lập hợp đồng hoặc văn bản chuyển giao ràng buộc trách nhiệm bảo vệ dữ liệu cá nhân giữa bên chuyển và bên nhận dữ liệu xuyên biên giới, không xác định rõ trách nhiệm thực hiện quyền của chủ thể dữ liệu cá nhân sau khi dữ liệu được chuyển; • Không bảo đảm sự đồng ý của chủ thể dữ liệu cá nhân đối với mục đích chuyển dữ liệu xuyên biên giới hoặc không thông báo cho chủ thể dữ liệu cá nhân về việc dữ liệu của họ được chuyển ra nước ngoài, tổ chức nhận dữ liệu và mục đích xử lý; • Không áp dụng biện pháp bảo mật phù hợp trong quá trình chuyển dữ liệu cá nhân xuyên biên giới hoặc không có phương án bảo đảm an toàn dữ liệu cá nhân sau khi chuyển ...
1% đến **2%** doanh thu năm tài chính liền trước tại thị trường Việt Nam	• Hành vi dẫn đến lộ, mất dữ liệu cá nhân của từ 10.000 đến dưới 100.000 chủ thể dữ liệu cá nhân là công dân Việt Nam.
2% đến **3%** doanh thu năm tài chính liền trước tại thị trường Việt Nam	• Hành vi dẫn đến lộ, mất dữ liệu cá nhân của từ 100.000 đến dưới 1.000.000 chủ thể dữ liệu cá nhân là công dân Việt Nam
3% đến **5%** doanh thu năm tài chính liền trước tại thị trường Việt Nam	• Hành vi dẫn đến lộ, mất dữ liệu cá nhân của từ 1.000.000 chủ thể dữ liệu cá nhân trở lên, hoặc hành vi chuyển dữ liệu cá nhân xuyên biên giới sau khi có quyết định yêu cầu ngừng chuyển của cơ quan chuyên trách bảo vệ dữ liệu cá nhân gây tổn hại đến quốc phòng, an ninh quốc gia ... và một số trường hợp cụ thể khác.

PHẦN 2: DOANH NGHIỆP CẦN LÀM GÌ KHI CÓ HOẠT ĐỘNG CHUYỂN DỮ LIỆU CÁ NHÂN XUYÊN BIÊN GIỚI?

Như vậy, trong trường hợp doanh nghiệp đã xác định được việc sử dụng dịch vụ điện toán đám mây là hoạt động chuyển dữ liệu xuyên biên giới, doanh nghiệp cần thực hiện các bước tuân thủ cần thiết theo quy định pháp luật để tránh bị phạt.

CDLAF

YOUR CONFIDANT

HỆ SINH THÁI CỦA CHÚNG TÔI

invest

CHO THUÊ VĂN PHÒNG

CFT

TUÂN THỦ DOANH NGHIỆP

Trụ sở: Phòng 7.01, Toà nhà Transimex, 172 Hai Bà Trưng, Phường Tân Định, Thành phố Hồ Chí Minh.

Chi nhánh: 330 Nguyễn Văn Trỗi, Phường Phú Lợi, Thành phố Hồ Chí Minh.

Văn phòng Giao dịch: 101/20 đường 11, Phường Thủ Đức, Thành phố Hồ Chí Minh.

info@cdlaf.vn +84 909 668 216 cdlaf.vn | /cdlaflawfirm