Trách Nhiệm của Bên Cung Cấp và Thỏa Thuận Xử Lý Dữ Liệu Theo Khung Pháp Lý về Bảo Vệ Dữ Liệu Cá Nhân của Việt Nam

RUSSIN & VECCHI – 2026

Lê Tôn Việt
Luật Sư Cao Cấp
Văn phòng tại Hà Nội

LTViet@russinvecchi.com.vn

TÓM TẮT

01	Bên kiểm soát dữ liệu chịu trách nhiệm cuối cùng đối với bất kỳ vi phạm nào xảy ra trong quá trình xử lý dữ liệu.
02	Thỏa thuận xử lý dữ liệu là một công cụ để quản lý các bên cung cấp và đặt ra các nghĩa vụ và trách nhiệm của các bên cung cấp.
03	Thỏa thuận xử lý dữ liệu phải bao gồm phạm vi xử lý, mục đích cụ thể, nghĩa vụ bảo mật, thông báo vi phạm và bồi thường.
04	Việc soạn thảo Thỏa thuận xử lý dữ liệu cần cân nhắc những rủi ro vận hành cụ thể.
05	Việc xác nhận rằng nhà cung cấp có áp dụng các biện pháp thích hợp để bảo vệ dữ liệu cá nhân hay không có thể được thực hiện qua hình thức kiểm tra hoặc tự đánh giá

Các quy định hiện hành về bảo vệ dữ liệu cá nhân

Đã hết hiệu lực:
Nghị định 13/2023/NĐ-CP
(Tình trạng: Bãi bỏ ngày 1 tháng 1 năm 2026)

→

Khung pháp lý hiện hành:
Luật số 91/2025/QH15 và Nghị định 356/2025/NĐ-CP
(Tình trạng: Có hiệu lực từ ngày 1 tháng 1 năm 2026)

- Luật Bảo vệ dữ liệu cá nhân mới (Luật 91) và Nghị định 356 đã có hiệu lực được 6+ tháng.

- Các quy định mới và Nghị định 13 có một số điểm tương đồng nhưng các yêu cầu tuân thủ theo các quy định mới đã được nâng cao hơn.

VAI TRÒ CỦA BÊN CUNG CẤP

Bên kiểm soát dữ liệu cá nhân

Quyết định mục đích và phương thức xử lý dữ liệu cá nhân.

Bên xử lý dữ liệu cá nhân

Xử lý dữ liệu cá nhân cho và thay mặt cho Bên kiểm soát dữ liệu, phù hợp với thỏa thuận giữa các bên.

Bên thứ ba

Bất kỳ bên nào - không phải là Bên xử lý dữ liệu hoặc Chủ thể dữ liệu- thực hiện một hoặc một số hoạt động xử lý dữ liệu cá nhân.

BÊN CUNG CẤP

Các bên cung cấp thường đảm nhiệm vai trò là Bên xử lý dữ liệu cá nhân; tuy nhiên, trong một số trường hợp nhất định, họ cũng có thể đóng vai trò là Bên kiểm soát dữ liệu cá nhân..

TRÁCH NHIỆM PHÁP LÝ CỦA BÊN KIỂM SOÁT DỮ LIỆU

Luồng dữ liệu

Trách nhiệm pháp lý

- Bên kiểm soát dữ liệu chịu trách nhiệm trực tiếp trước cơ quan có thẩm quyền (Cục an ninh mạng và phòng chống tội phạm công nghệ cao A05 – Bộ Công An) và Chủ thể dữ liệu, bất kể vi phạm kỹ thuật xảy ra ở đâu.

- Theo Luật 91 và Nghị định 356, Bên kiểm soát phải chứng minh rằng Chủ thể dữ liệu đã đồng ý hợp lệ đối với các hoạt động xử lý cụ thể của bên cung cấp.

THỎA THUẬN XỬ LÝ DỮ LIỆU CÁ NHÂN

- Pháp luật không có yêu cầu cụ thể về nội dung của thỏa thuận xử lý dữ liệu cá nhân.
- Thỏa thuận xử lý dữ liệu cá nhân hoặc bất kỳ thỏa thuận nào khác giữa Bên kiểm soát và Bên xử lý liên quan đến việc xử lý dữ liệu cá nhân cần phải bao gồm:
  - **Phạm vi và thời gian:** Danh mục dữ liệu và thời gian xử lý được xác định rõ ràng.
  - **Mục đích cụ thể:** Phù hợp chặt chẽ với sự đồng ý của chủ thể dữ liệu.
  - **Nghĩa vụ bảo mật:** Cam kết về các biện pháp kỹ thuật và tổ chức.
  - **Quy trình xử lý vi phạm:** Hợp tác giữa ben kiểm soát và bên xử lý để thông báo.
  - **Chấm dứt:** Quy trình cụ thể để trả lại hoặc hủy dữ liệu.

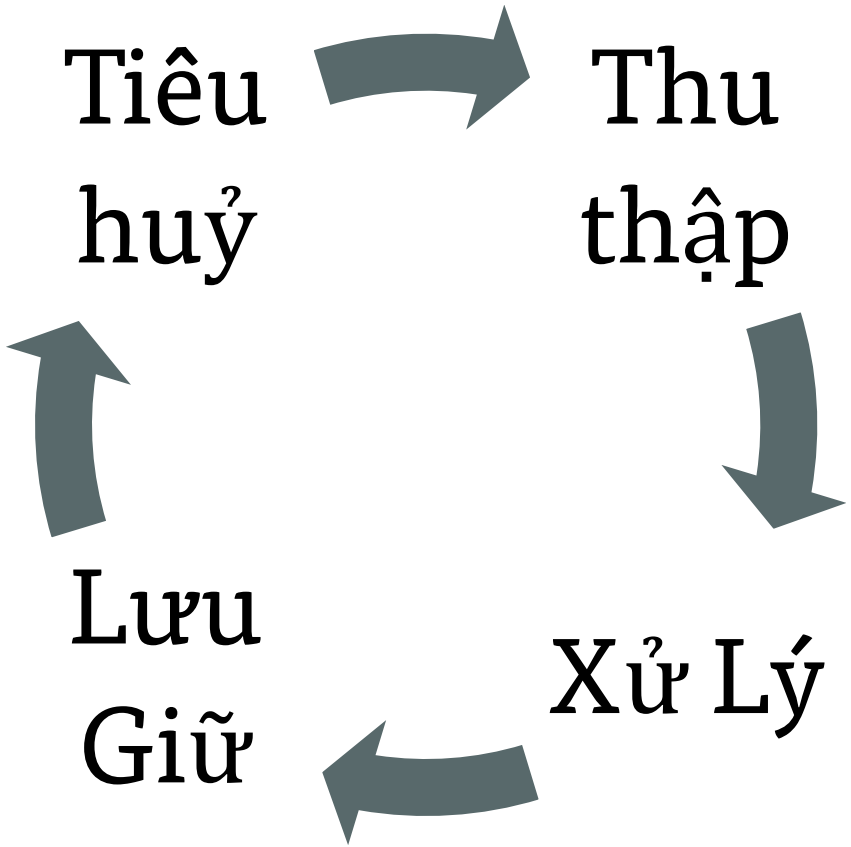
Giới Hạn Mục Đích

- Phạm vi xử lý dữ liệu được xác định rõ ràng.
- Thỏa thuận xử lý dữ liệu không được cho phép các bên cung cấp bổ sung các mục đích xử lý dữ liệu chung như nghiên cứu thị trường, cải tiến dịch vụ, v.v. Nếu những mục đích này được cho phép, DPA phải yêu cầu bên cung cấp ẩn danh dữ liệu cá nhân có liên quan. Việc ẩn danh phải được thực hiện theo Luật 91.
- Việc xử lý dữ liệu được ngoài phạm vi đã được xác định phải được thỏa thuận bằng văn bản và phải được sự đồng ý của chủ thể dữ liệu.

Tiêu Chuẩn Bảo Mật

- **Mã hóa:** Dữ liệu phải được mã hóa trong quá trình lưu trữ và chuyển giao.
- **Kiểm soát truy cập:** Xác thực đa yếu tố và truy cập “Quyền tối thiểu".
- **Ghi nhật ký:** Nhật ký truy cập hệ thống phải được lưu giữ tối thiểu 12 tháng.

LƯU GIỮ VÀ TIÊU HUỶ DỮ LIỆU



- **Quyền được lãng quên:** Chủ thể dữ liệu có thể yêu cầu xoá dữ liệu của họ hoặc rút lại sự đồng ý.
- **Khi chấm dứt hợp đồng xử lý dữ liệu:** Dữ liệu phải được hoàn trả hoặc huỷ bỏ. Các bên thoả thuận trong trường hợp phải có Chứng Nhận Tiêu Huỷ.
- **Mâu thuẫn Lưu Giữ Dữ Liệu:** Một bên cung cấp có được lưu giữ dữ liệu cho các mục đích thuế hay tuân thủ hay không?

Rủi ro vận hành trong quan hệ với Bên Cung Cấp

1

Chuyển dữ liệu xuyên biên giới

Khi bên cung cấp thực hiện chuyển dữ liệu cá nhân qua biên giới theo Luật Bảo vệ dữ liệu cá nhân, các yêu cầu liên quan đến việc chuyển dữ liệu cá nhân xuyên biên giới sẽ được kích hoạt

2

Thông báo vi phạm quy định xử lý dữ liệu

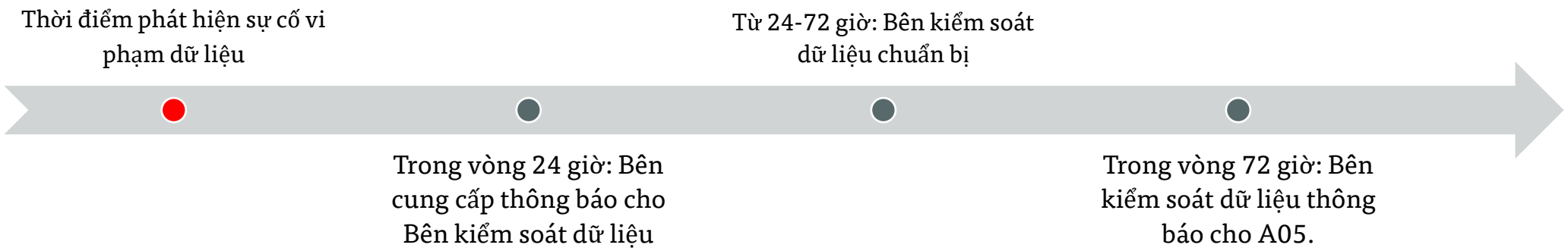
Thời hạn luật định để nộp thông báo vi phạm với cơ quan có thẩm quyền là 72 giờ sau khi phát hiện vi phạm (bao gồm cả trường hợp bên phát hiện ra vi phạm là bên cung cấp.

3

Thực hiện yêu cầu của chủ thể dữ liệu

Bên cung cấp phải có năng lực kỹ thuật để xóa, hạn chế hoặc cung cấp dữ liệu trong các thời hạn luật định, theo yêu cầu của chủ thể dữ liệu

Yêu Cầu Thông Báo Vi Phạm



- Trong vòng 72 giờ kể từ khi phát hiện vi phạm dữ liệu, Bên kiểm soát dữ liệu phải thông báo cho A05 sử dụng biểu mẫu quy định tại Nghị Định 356. Nếu sự cố vi phạm dữ liệu có liên quan đến một số loại dữ liệu cá nhân nhất định (ví dụ, dữ liệu sinh trắc học), Bên kiểm soát dữ liệu cũng phải thông báo cho chủ thể dữ liệu theo quy định tại Nghị Định 356.

- Các thông tin sau đây phải được bao gồm trong thông báo:
  - Mô tả sự việc;
  - Thiệt hại và hậu quả có thể xảy ra;
  - Thông tin của nhân sự bảo vệ dữ liệu;
  - Các biện pháp đang được thực hiện để giảm thiểu hoặc khắc phục tình hình.

Xử Lý Yêu Cầu Của Chủ Thể Dữ Liệu

Quy trình xử lý yêu cầu

Loại yêu cầu	Thời gian phản hồi	Thời gian thực hiện
Để rút lại sự đồng ý	2 ngày làm việc	15 ngày hoặc 20 ngày nếu có bên xử lý dữ liệu
Xem, chỉnh sửa hoặc cập nhật dữ liệu cá nhân	2 ngày làm việc	10 ngày hoặc 15 ngày nếu có bộ xử lý dữ liệu
Cách xóa dữ liệu cá nhân	2 ngày làm việc	20 ngày hoặc 30 ngày nếu có bộ xử lý dữ liệu
Để thực hiện các biện pháp bảo vệ	2 ngày làm việc	15 ngày

Quyền Kiểm Tra Đánh Giá

- Vì Bên kiểm soát dữ liệu chịu trách nhiệm cuối cùng về tất cả các hoạt động xử lý dữ liệu, Bên kiểm soát dữ liệu cũng sẽ chịu trách nhiệm về việc tuân thủ của Bên xử lý dữ liệu.

- Đề xuất áp dụng kiểm tra đánh giá hai cấp:
  - **Bảng câu hỏi:** Bảng câu hỏi tự đánh giá do Bên xử lý dữ liệu trả lời và trong một số trường hợp nhất định, có thể yêu cầu chứng chỉ SOC2/ISO 27001;
  - **Kiểm tra trực tiếp:** Dành riêng cho các bên cung cấp có rủi ro cao hoặc sau khi xảy ra vi phạm.

- Bên kiểm soát dữ liệu có thể yêu cầu Bên xử lý chịu chi phí kiểm tra nếu phát hiện ra bất kỳ vi phạm tuân thủ quan trọng nào.

Ví Dụ - Câu Hỏi Kiểm Tra Đánh Giá

Các câu hỏi đánh giá thường tập trung vào một số các khía cạnh chính:

- **Chính sách:** Bên xử lý có các chính sách / quy trình cụ thể nào liên quan đến xử lý dữ liệu cá nhân? (ví dụ: chính sách quyền riêng tư hoặc chính sách quản lý lỗ hổng bảo mật).

- **Đánh giá bảo mật dữ liệu công nghệ thông tin:** Trong vòng 12 tháng gần nhất, bên xử lý đã thực hiện đánh giá SOC 2 đã được thực hiện với các quy trình và kiểm soát bảo mật chưa? Bên xử lý đã thực hiện Báo Cáo Đánh giá lỗ hổng bảo mật và Kiểm tra thâm nhập hay chưa?

- **Đánh giá quy trình quản lý:** Tổ chức có chia tách mạng theo nhóm dịch vụ thông tin, người dùng và hệ thống thông tin không? Phương pháp nào được sử dụng để phá hủy dữ liệu được lưu trữ trên băng, đĩa cứng và các phương tiện điện tử khác để đảm bảo dữ liệu hoàn toàn không thể đọc được, không thể sử dụng được và không thể truy cập lại được?

Phạt và Bồi Thường Thiệt Hại

- Các quy định về phạt và bồi thường thiệt hại vi phạm Thỏa thuận xử lý dữ liệu vẫn tuân theo các quy tắc về phạt và bồi thường trong hợp đồng thương mại/dân sự thông thường.

- Các khoản bồi thường thiệt hại được định trước có thể được tòa án chấp nhận nhưng trên thực tế vẫn còn nhiều vấn đề tồn đọng trong việc áp dụng và thực thi bồi thường thiệt hại được định trước.