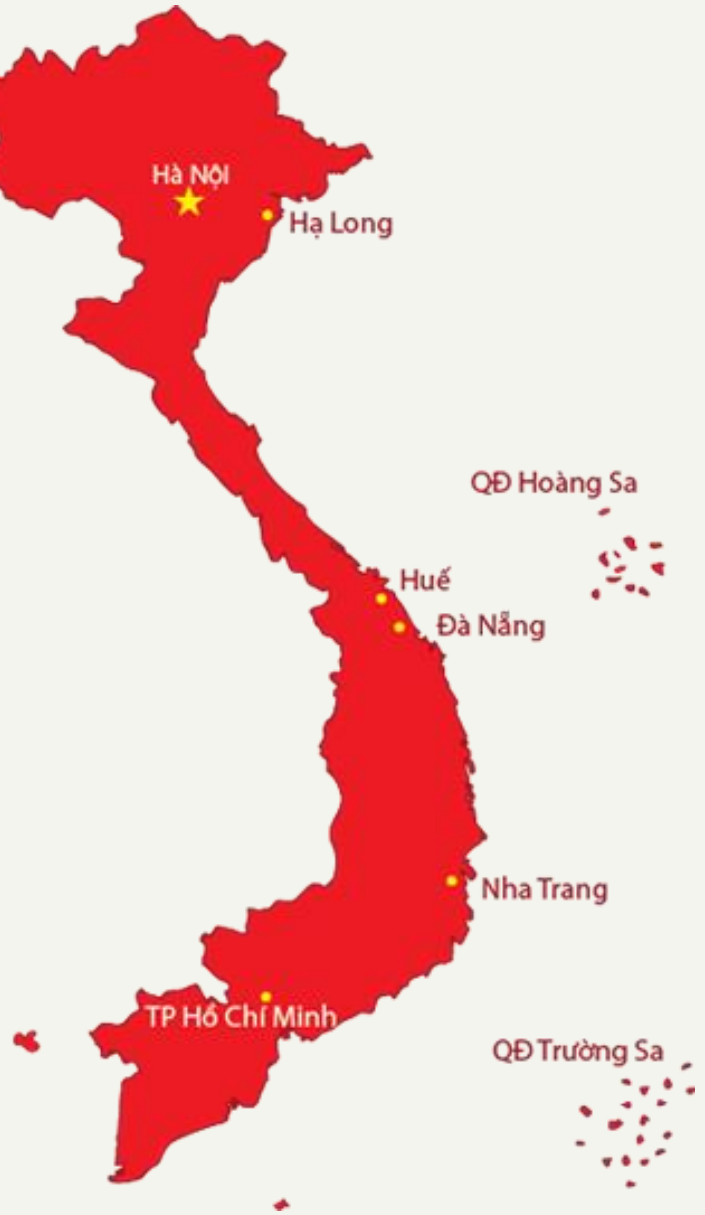
Danh Mục Kiểm Tra Tuân Thủ - Luật Bảo Vệ Dữ Liệu Cá Nhân Của Việt Nam

Lê Tôn Việt
RUSSIN & VECCHI

Tel: (84-24) 3825-1700
Email: LTViet@russinvecchi.com.vn
Web: www.russinvecchi.com.vn

Đối tượng áp dụng

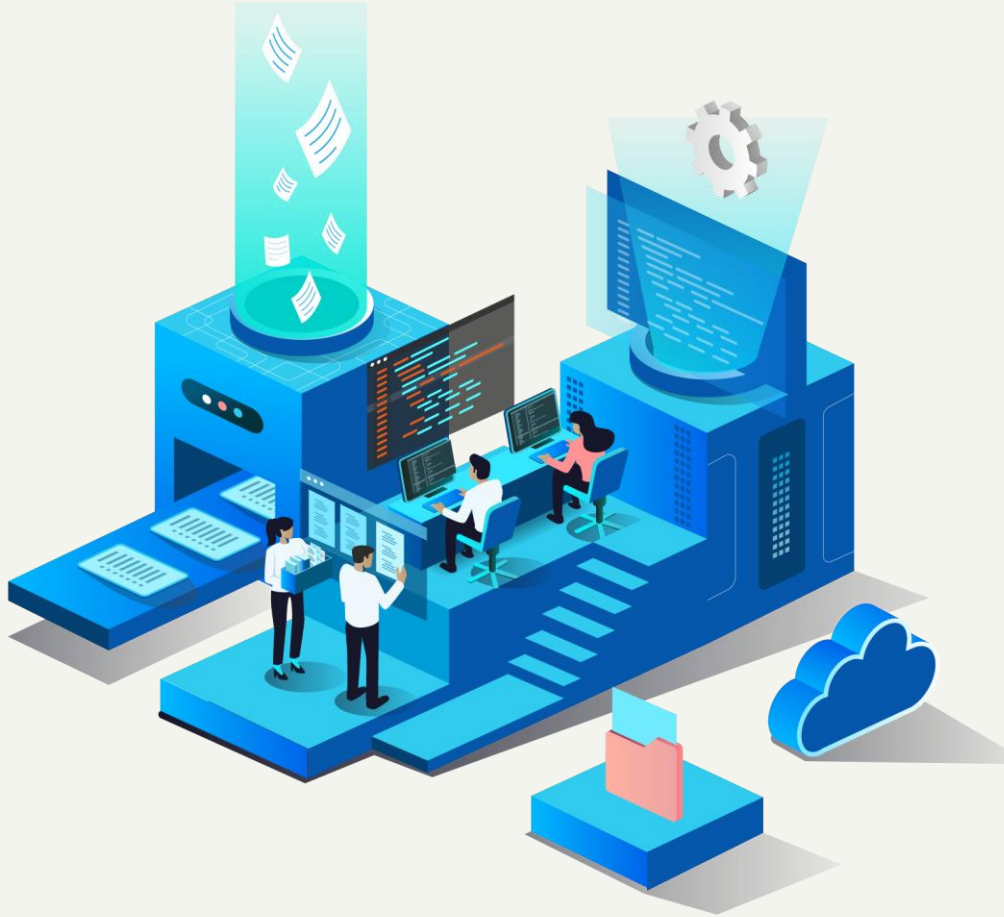
- **Tổ chức có được thành lập và hoạt động tại Việt Nam không?**
- Nếu câu trả lời là 'có' và tổ chức xử lý dữ liệu cá nhân của bất kỳ chủ thể dữ liệu nào, các quy định bảo vệ dữ liệu cá nhân của Việt Nam sẽ được áp dụng.
- **Tổ chức có xử lý dữ liệu của công dân Việt Nam hoặc người gốc Việt Nam đang cư trú tại Việt Nam không?**
- Nếu câu trả lời là 'có', các quy định bảo vệ dữ liệu cá nhân của Việt Nam sẽ được áp dụng bất kể tổ chức ở nước ngoài hay ở trong nước**.**



Hoạt động xử lý dữ liệu cá nhân là gì?

Bất kỳ hành động nào ảnh hưởng đến dữ liệu cá nhân:

SƯU TẬP	TIẾT LỘ	PHÂN TÍCH	XÓA
MÃ HÓA	CHUYỂN GIAO	KẾT HỢP	THAY ĐỔI
GIẢI MÃ	KHỬ NHẬN DẠNG	CÁC HOẠT ĐỘNG KHÁC LIÊN QUAN ĐẾN DỮ LIỆU CÁ NHÂN	



VAI TRÒ CỦA TỔ CHỨC

Một tổ chức có thể đảm nhận một hoặc nhiều vai trò này tùy thuộc vào loại giao dịch. Ví dụ: tổ chức có thể vừa là bên kiểm soát dữ liệu vừa là bên xử lý dữ liệu liên quan đến dữ liệu cá nhân của nhân viên. Một tổ chức cũng có thể là đơn vị xử lý dữ liệu cho một tổ chức khác.

Công Ty cần phải hiểu vai trò của mình liên quan đến từng loại dữ liệu cá nhân liên quan và trong mỗi giao dịch.

Bên kiểm soát dữ liệu

Một tổ chức hoặc cá nhân xác định mục đích và cách thức xử lý dữ liệu cá nhân.

Bên xử lý dữ liệu

Bất kỳ tổ chức hoặc cá nhân nào xử lý dữ liệu cá nhân cho và thay mặt cho bên kiểm soát dữ liệu theo thỏa thuận.

Bên thứ ba

Bất kỳ bên nào khác tham gia vào một số hoạt động xử lý mà không phải là bên xử lý dữ liệu hoặc chủ thể dữ liệu.

Dữ liệu cá nhân cơ bản

- Họ, chữ đệm và tên khai sinh, tên gọi khác (nếu có);
- Ngày, tháng, năm sinh; ngày, tháng, năm chết hoặc mất tích;
- Giới tính;
- Nơi sinh, nơi đăng ký khai sinh, nơi đăng ký thường trú, nơi đăng ký tạm trú, nơi ở hiện tại, quê quán, địa chỉ liên hệ;
- Quốc tịch;
- Hình ảnh của cá nhân;
- Số điện thoại, số định danh cá nhân, số hộ chiếu, số giấy phép lái xe, số biển số xe;
- Tình trạng hôn nhân;
- Thông tin về mối quan hệ gia đình (cha mẹ, con, vợ, chồng);
- Thông tin về tài khoản số của cá nhân;
- Các thông tin khác gắn liền với một con người cụ thể hoặc giúp xác định một con người cụ thể mà không phải là dữ liệu cá nhân nhạy cảm

Dữ liệu cá nhân nhạy cảm

- Dữ liệu tiết lộ nguồn gốc chủng tộc, dân tộc;
- Quan điểm về chính trị, tôn giáo, tín ngưỡng;
- Thông tin đời sống riêng tư, bí mật cá nhân, gia đình;
- Tình trạng sức khỏe;
- Dữ liệu sinh trắc học, đặc điểm di truyền;
- Dữ liệu tiết lộ đời sống tình dục, xu hướng tình dục;
- Dữ liệu về tội phạm, vi phạm pháp luật được thu thập, lưu trữ bởi các cơ quan thực thi pháp luật;
- Vị trí của cá nhân được xác định qua dịch vụ định vị;
- Thông tin tên đăng nhập và mật khẩu VNeID; hình ảnh thẻ căn cước,;
- Tên đăng nhập, mật khẩu tài khoản ngân hàng; thông tin thẻ ngân hàng, dữ liệu về lịch sử giao dịch; thông tin tài chính, tín dụng và các thông tin về hoạt động, lịch sử giao dịch của khách hàng tại các tổ chức được phép;
- Dữ liệu theo dõi hành vi, hoạt động trên không gian mạng;
- Dữ liệu cá nhân khác được pháp luật quy định cần giữ bí mật hoặc cần có biện pháp bảo mật chặt chẽ.

Quyền của chủ thể dữ liệu

01	Quyền được biết về hoạt động xử lý
02	Quyền đưa ra hoặc rút lại sự đồng ý
03	Quyền xem và điều chỉnh
04	Quyền yêu cầu sao chép, xóa hoặc hạn chế xử lý dữ liệu
05	Quyền yêu cầu cơ quan có thẩm quyền hoặc các bên liên quan thực hiện các biện pháp pháp lý liên quan đến dữ liệu cá nhân

Nghĩa vụ của chủ thể dữ liệu

01	Bảo vệ dữ liệu cá nhân của chính mình
02	Tôn trọng và bảo vệ dữ liệu cá nhân của người khác
03	Cung cấp dữ liệu cá nhân đầy đủ và chính xác
04	Tuân thủ các quy định về dữ liệu cá nhân

Cơ sở pháp lý để xử lý dữ liệu cá nhân

- **Sự đồng ý**
- Bảo vệ tính mạng, sức khỏe, uy tín, nhân phẩm, quyền và lợi ích hợp pháp của chủ thể dữ liệu hoặc người khác trong trường hợp khẩn cấp; bảo vệ quyền và lợi ích hợp pháp của cá nhân, lợi ích của chính quyền, tổ chức trước các hành vi vi phạm;
- Xử lý dữ liệu cá nhân trong trường hợp khẩn cấp về quốc phòng, an ninh quốc gia, trật tự an toàn xã hội, thiên tai, dịch bệnh; hoặc các nguy cơ tiềm ẩn đối với an ninh quốc gia nhưng không bắt buộc phải tuyên bố tình trạng khẩn cấp; hoặc để chống bạo loạn, khủng bố, tội phạm, v.v.;
- Thực hiện nghĩa vụ hợp đồng của chủ thể dữ liệu đối với các tổ chức, cá nhân có liên quan theo quy định của pháp luật;
- Để phục vụ hoạt động của các cơ quan chức năng theo quy định

Sự đồng ý

1

Tự nguyện và đầy đủ thông tin

Sự đồng ý phải tự nguyện và được thông báo đầy đủ về loại dữ liệu cá nhân được xử lý, mục đích xử lý, ai được phép xử lý và quyền và nghĩa vụ của chủ thể dữ liệu và liệu dữ liệu đó có phải là dữ liệu cá nhân nhạy cảm hay không.

2

Rõ ràng và cụ thể

Sự đồng ý phải được thể hiện rõ ràng và cụ thể bằng văn bản, ghi âm, đánh dấu đồng ý, tin nhắn văn bản, lựa chọn phương án kỹ thuật để đồng ý hoặc các hành động khác. Im lặng hoặc không hành động sẽ không được coi là sự đồng ý hợp lệ.

3

Có thể xác minh

Sự đồng ý phải ở định dạng có thể được in, sao chép bằng văn bản, bao gồm các định dạng điện tử và các định dạng có thể xác minh khác.

4

Yêu cầu bổ sung

Có thể đồng ý một phần hoặc với điều kiện nhất định.

Tổ chức có cung cấp bất kỳ dịch vụ nào sau đây cho bên thứ ba không? Nếu có, tổ chức phải tuân thủ các quy định được thể hiện ở trang tiếp theo.

- Dịch vụ cung cấp và vận hành hệ thống, phần mềm tự động để thay mặt bên kiểm soát, bên kiểm soát và xử lý tiến hành xử lý dữ liệu cá nhân.
- Dịch vụ chấm điểm, xếp hạng, đánh giá mức độ tín nhiệm của chủ thể dữ liệu cá nhân.
- Dịch vụ thu thập, xử lý dữ liệu cá nhân trực tuyến từ trang web, ứng dụng, phần mềm và mạng xã hội.
- Dịch vụ thu thập, xử lý dữ liệu cá nhân qua trang web, ứng dụng, phần mềm chăm sóc sức khỏe, theo dõi sức khỏe, dịch vụ y tế.
- Dịch vụ thu thập, xử lý dữ liệu cá nhân qua ứng dụng, phần mềm giáo dục có yếu tố giám sát như điểm danh, ghi hình, chấm điểm hành vi, nhận diện cảm xúc.
- Dịch vụ phân tích và khai thác dữ liệu cá nhân, gồm: sử dụng các công cụ phân tích để tìm kiếm thông tin, xu hướng và mẫu từ dữ liệu cá nhân; áp dụng các phương pháp khai thác dữ liệu để trích xuất giá trị từ dữ liệu cá nhân, dự đoán hành vi người dùng hoặc tối ưu hóa dịch vụ.
- Dịch vụ mã hóa dữ liệu cá nhân trong quá trình truyền tải và lưu trữ.
- Dịch vụ xử lý dữ liệu cá nhân tự động dựa trên công nghệ dữ liệu lớn, trí tuệ nhân tạo, chuỗi khối, vũ trụ ảo.
- Dịch vụ nền tảng ứng dụng cung cấp dữ liệu vị trí cá nhân..

Dịch vụ xử lý dữ liệu

Đơn vị cung cấp dịch vụ xử lý dữ liệu:

- Được thành lập và hoạt động hợp lệ tại Việt Nam
- Người đứng đầu phụ trách chuyên môn về xử lý dữ liệu cá nhân phải là người Việt Nam và phải cư trú tại Việt Nam;
- Ít nhất 3 nhân sự đủ điều kiện;
- Có cơ sở hạ tầng, trang thiết bị, cơ sở vật chất phù hợp;
- Đánh giá tác động xử lý dữ liệu và đánh giá tác động chuyển dữ liệu của đơn vị được coi là 'đạt yêu cầu'.

Nhân sự đủ điều kiện bao gồm::

- Có bằng đại học;
- Ít nhất 2 năm kinh nghiệm trong một trong các lĩnh vực: pháp lý, CNTT, an ninh mạng, bảo mật dữ liệu, quản lý rủi ro, tuân thủ, nhân sự;
- Đã được đào tạo kiến thức pháp lý và kỹ năng chuyên môn liên quan đến bảo vệ dữ liệu.

Thủ tục cấp phép:

- Thuộc thẩm quyền của Bộ Công an;
- Tài liệu bao gồm một Đề án đề nghị cấp Giấy chứng nhận đủ điều kiện kinh doanh dịch vụ xử lý dữ liệu cá nhân và các hồ sơ chứng minh;
- Thời gian theo luật định cho thủ tục này có thể lên đến 40 ngày.

Đánh giá tác động dữ liệu cá nhân

- **Tổ chức có chuyển dữ liệu đến một địa điểm bên ngoài Việt Nam không? (bao gồm sử dụng dịch vụ đám mây)**

Nếu câu trả lời là có, thì cần phải có Đánh giá tác động chuyển dữ liệu cá nhân qua biên giới.

- **Tổ chức có nộp đánh giá tác động theo quy định tại Nghị định 13/2023/NĐ-CP hay không?**

Nếu câu trả lời là có, không cần nộp mới, nhưng tổ chức sẽ phải cập nhật các đánh giá tác động theo quy định hiện hành.

- **Cơ quan có thẩm quyền đã phản hồi các đánh giá tác động đã gửi chưa?**

Nếu câu trả lời là không, vui lòng theo dõi với cơ quan có thẩm quyền;

- **Đã bao lâu kể từ khi các đánh giá tác động được nộp cho cơ quan có thẩm quyền?**

Đánh giá tác động được yêu cầu cập nhật sáu tháng một lần hoặc ngay lập tức trong một số trường hợp nhất định.

Nhân sự bảo vệ dữ liệu hoặc DPO

Nhân viên bảo vệ dữ liệu:

- Có thể được tuyển dụng hoặc thuê ngoài;
- Có thể được miễn trách nhiệm theo thỏa thuận trong một số trường hợp nhất định.

Danh sách tài liệu hỗ trợ:

- Quyết định bổ nhiệm;
- Bản sao các bằng cấp và bằng cấp liên quan;
- Thông tin liên hệ.

Nhân sự đủ điều kiện:

- Có bằng đại học;
- Ít nhất 2 năm (3 năm nếu thuê ngoài) kinh nghiệm ở một trong các lĩnh vực: pháp lý, CNTT, an ninh mạng, bảo mật dữ liệu, quản lý rủi ro, tuân thủ, nhân sự;
- Đã được đào tạo về kiến thức pháp lý và kỹ năng chuyên môn liên quan đến bảo vệ dữ liệu.

Tổ chức cung cấp dịch vụ bảo vệ dữ liệu:

- Phải có ngành nghề kinh doanh phù hợp (CNTT, pháp lý hoặc tư vấn));
- Phải có ít nhất 3 nhân sự đủ điều kiệnl;
- Phải có một hồ sơ doanh nghiệp thể hiện năng lực của tổ chức.

Cân nhắc bổ sung

Tổ chức có hoạt động trong bất kỳ lĩnh vực kinh doanh nào sau đây: AI, blockchain, metaverse, điện toán đám mây, quảng cáo, tài chính, bảo hiểm không. Nếu có, tổ chức sẽ phải cân nhắc các quy định bổ sung.

Tổ chức có tổ chức đào tạo cho nhân viên của mình về bảo vệ dữ liệu cá nhân không? Câu trả lời phải là có và việc đào tạo phải được ghi chép lại.

Tổ chức có kế hoạch ứng phó vi phạm, Chính sách bảo mật, Chính sách bảo mật thông tin, Phân loại dữ liệu, Kế hoạch đào tạo không? Câu trả lời phải là có.

Danh mục kiểm tra tuân thủ ngắn gọn

01	Đã có được sự đồng ý của chủ thể dữ liệu đúng cách
02	Các đánh giá tác động đã gửi sẽ được chuyển tiếp. Các đánh giá tác động sẽ được cơ quan có thẩm quyền xem xét và được coi là 'đạt yêu cầu' hoặc 'không đạt yêu cầu'.
03	Có những quy địnhmới liên quan đến nhân viên bảo vệ dữ liệu.
04	Có những quy định mới liên quan đến dịch vụ xử lý dữ liệu.
05	Tổ chức phải có các biện pháp thích hợp để bảo vệ dữ liệu cá nhân. Các biện pháp này phải được lập thành văn bản và phổ biến cho nhân viên của tổ chức.