

Số: 356/2025/NĐ-CP

Hà Nội, ngày 31 tháng 12 năm 2025

NGHỊ ĐỊNH
Quy định chi tiết một số điều và biện pháp thi hành
Luật Bảo vệ dữ liệu cá nhân

Căn cứ Luật Tổ chức Chính phủ số 63/2025/QH15;

Căn cứ Luật Bảo vệ dữ liệu cá nhân số 91/2025/QH15;

Căn cứ Luật Dữ liệu số 60/2024/QH15;

Căn cứ Luật sửa đổi, bổ sung một số điều của Luật Đầu thầu, Luật Đầu tư theo phương thức đối tác công tư, Luật Hải quan, Luật Thuế giá trị gia tăng, Luật Thuế xuất khẩu, thuế nhập khẩu, Luật Đầu tư, Luật Đầu tư công, Luật quản lý sử dụng tài sản công số 90/2025/QH15;

Theo đề nghị của Bộ trưởng Bộ Công an;

Chính phủ ban hành Nghị định quy định chi tiết một số điều và biện pháp thi hành Luật Bảo vệ dữ liệu cá nhân.

Chương I
QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh

Nghị định này quy định chi tiết khoản 2, khoản 3 Điều 2; khoản 5 Điều 4; khoản 3 Điều 6; khoản 5 Điều 9; khoản 3 Điều 17; khoản 7 Điều 20; khoản 7 Điều 21; khoản 4 Điều 22; khoản 5 Điều 23; khoản 3 Điều 27; khoản 6 Điều 30; điểm b khoản 4 Điều 31; khoản 3 Điều 33; Điều 35; khoản 4 Điều 38 Luật Bảo vệ dữ liệu cá nhân và quy định các biện pháp để tổ chức thi hành Luật về nghiên cứu, phát triển các giải pháp bảo vệ dữ liệu cá nhân, cơ quan chuyên trách bảo vệ dữ liệu cá nhân, Công thông tin quốc gia về bảo vệ dữ liệu cá nhân; trách nhiệm của các bộ, ngành, địa phương trong bảo vệ dữ liệu cá nhân; kinh phí bảo đảm hoạt động bảo vệ dữ liệu cá nhân.

Điều 2. Đối tượng áp dụng

1. Cơ quan, tổ chức, cá nhân Việt Nam;
2. Cơ quan, tổ chức, cá nhân nước ngoài tại Việt Nam;
3. Cơ quan, tổ chức, cá nhân nước ngoài trực tiếp tham gia hoặc có liên quan đến hoạt động xử lý dữ liệu cá nhân của công dân Việt Nam và người gốc Việt Nam chưa xác định được quốc tịch đang sinh sống tại Việt Nam đã được cấp giấy chứng nhận căn cước.

Điều 3. Danh mục dữ liệu cá nhân cơ bản

Dữ liệu cá nhân cơ bản bao gồm:

1. Họ, chữ đệm và tên khai sinh, tên gọi khác (nếu có);
2. Ngày, tháng, năm sinh; ngày, tháng, năm chết hoặc mất tích;
3. Giới tính;
4. 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;
5. Quốc tịch;
6. Hình ảnh của cá nhân;
7. Số điện thoại, số định danh cá nhân, số hộ chiếu, số giấy phép lái xe, số biển số xe;
8. Tình trạng hôn nhân;
9. Thông tin về mối quan hệ gia đình (cha mẹ, con, vợ, chồng);
10. Thông tin về tài khoản số của cá nhân;
11. Các thông tin khác gắn liền với một con người cụ thể hoặc giúp xác định một con người cụ thể không thuộc quy định tại Điều 4 Nghị định này.

Điều 4. Danh mục dữ liệu cá nhân nhạy cảm

1. Dữ liệu cá nhân nhạy cảm bao gồm:
 - a) Dữ liệu tiết lộ nguồn gốc chủng tộc, nguồn gốc dân tộc;
 - b) Quan điểm về chính trị, tôn giáo, tín ngưỡng;

- c) Thông tin về đời sống riêng tư, bí mật cá nhân, bí mật gia đình;
- d) Tình trạng sức khỏe;
- đ) Dữ liệu sinh trắc học, đặc điểm di truyền;
- e) Dữ liệu tiết lộ đời sống tình dục, xu hướng tình dục của cá nhân;
- g) Dữ liệu về tội phạm, vi phạm pháp luật được thu thập, lưu trữ bởi các cơ quan thực thi pháp luật;
- h) Vị trí của cá nhân được xác định qua dịch vụ định vị;
- i) Thông tin tên đăng nhập và mật khẩu truy cập tài khoản định danh điện tử của cá nhân; hình ảnh thẻ căn cước, thẻ căn cước công dân, chứng minh nhân dân;
- k) Tên đăng nhập, mật khẩu truy cập của tài khoản ngân hàng; thông tin thẻ ngân hàng, dữ liệu về lịch sử giao dịch của tài khoản ngân hàng; thông tin tài chính, tín dụng và các thông tin về hoạt động, lịch sử giao dịch tài chính, chứng khoán, bảo hiểm của khách hàng tại các tổ chức tín dụng, chi nhánh ngân hàng nước ngoài, tổ chức cung ứng dịch vụ trung gian thanh toán, chứng khoán, bảo hiểm, các tổ chức được phép khác;
- l) Dữ liệu theo dõi hành vi, hoạt động sử dụng dịch vụ viễn thông, mạng xã hội, dịch vụ truyền thông trực tuyến và các dịch vụ khác trên không gian mạng;
- m) Dữ liệu cá nhân khác được pháp luật quy định cần giữ bí mật hoặc cần có biện pháp bảo mật chặt chẽ.

2. Trong quá trình xử lý dữ liệu cá nhân nhạy cảm, cơ quan, tổ chức phải thiết lập quy định phân quyền giới hạn truy cập, quy trình xử lý và các biện pháp bảo mật.

Chương II

YÊU CẦU, ĐIỀU KIỆN BẢO VỆ DỮ LIỆU CÁ NHÂN

Điều 5. Thực hiện quyền của chủ thể dữ liệu cá nhân

1. Bên kiểm soát dữ liệu cá nhân, bên kiểm soát và xử lý dữ liệu cá nhân phải xây dựng quy trình, thủ tục, biểu mẫu rõ ràng để thực hiện các quyền của chủ thể dữ liệu cá nhân phù hợp với hoạt động xử lý dữ liệu cá nhân và trách nhiệm các bộ phận có liên quan; đảm bảo chủ thể dữ liệu cá nhân được biết về

thủ tục thực hiện các quyền quy định tại khoản 1 Điều 4 của Luật Bảo vệ dữ liệu cá nhân.

2. Khi nhận được yêu cầu rút lại sự đồng ý cho phép xử lý dữ liệu cá nhân, hạn chế xử lý dữ liệu cá nhân, phản đối xử lý dữ liệu cá nhân theo đúng thủ tục của chủ thể dữ liệu cá nhân, bên kiểm soát dữ liệu cá nhân, bên kiểm soát và xử lý dữ liệu cá nhân phải phản hồi trong thời hạn 02 ngày làm việc, cung cấp đầy đủ thông tin cho chủ thể dữ liệu cá nhân về thủ tục ngừng xử lý dữ liệu cá nhân và thực hiện trong thời hạn 15 ngày, trừ trường hợp xử lý dữ liệu cá nhân không cần sự đồng ý của chủ thể dữ liệu cá nhân theo quy định tại Điều 19 Luật Bảo vệ dữ liệu cá nhân. Trường hợp cần yêu cầu bên xử lý dữ liệu cá nhân, bên thứ ba ngừng xử lý dữ liệu cá nhân của chủ thể dữ liệu cá nhân thì thực hiện trong thời hạn 20 ngày.

Tùy theo tính chất, mức độ phức tạp của yêu cầu, trường hợp cần gia hạn thời gian xử lý thì kéo dài thêm tối đa 01 lần gia hạn trong thời hạn không quá 15 ngày, bên kiểm soát dữ liệu cá nhân, bên kiểm soát và xử lý dữ liệu cá nhân thông báo cho chủ thể dữ liệu cá nhân lý do cần gia hạn và chịu trách nhiệm chứng minh việc gia hạn là cần thiết, hợp lý.

3. Khi nhận được yêu cầu xem, chỉnh sửa hoặc yêu cầu chỉnh sửa dữ liệu cá nhân, cung cấp dữ liệu cá nhân theo đúng thủ tục của chủ thể dữ liệu cá nhân, bên kiểm soát dữ liệu cá nhân, bên kiểm soát và xử lý dữ liệu cá nhân phải phản hồi trong thời hạn 02 ngày làm việc, cung cấp đầy đủ thông tin cho chủ thể dữ liệu cá nhân về thủ tục và thực hiện trong thời hạn 10 ngày. Trường hợp cần yêu cầu bên xử lý dữ liệu cá nhân, bên thứ ba chỉnh sửa dữ liệu cá nhân của chủ thể dữ liệu cá nhân thì thực hiện trong thời hạn 15 ngày.

Tùy theo tính chất, mức độ phức tạp của yêu cầu, trường hợp cần gia hạn thời gian xử lý thì kéo dài thêm tối đa 01 lần gia hạn trong thời hạn không quá 10 ngày, bên kiểm soát dữ liệu cá nhân, bên kiểm soát và xử lý dữ liệu cá nhân thông báo cho chủ thể dữ liệu cá nhân lý do cần gia hạn và chịu trách nhiệm chứng minh việc gia hạn là cần thiết, hợp lý.

4. Khi nhận được yêu cầu xóa dữ liệu cá nhân theo đúng thủ tục của chủ thể dữ liệu cá nhân, bên kiểm soát dữ liệu cá nhân, bên kiểm soát và xử lý dữ

liệu cá nhân phải phản hồi trong thời hạn 02 ngày làm việc, cung cấp đầy đủ thông tin cho chủ thể dữ liệu cá nhân về thủ tục và thực hiện trong thời hạn 20 ngày. Trường hợp cần yêu cầu bên xử lý dữ liệu cá nhân, bên thứ ba cung cấp, xóa, hạn chế xử lý dữ liệu của chủ thể dữ liệu cá nhân thì thực hiện trong thời hạn 30 ngày.

Tùy theo tính chất, mức độ phức tạp của yêu cầu, trường hợp cần gia hạn thời gian xử lý thì kéo dài thêm tối đa 01 lần gia hạn trong thời hạn không quá 20 ngày, bên kiểm soát dữ liệu cá nhân, bên kiểm soát và xử lý dữ liệu cá nhân thông báo cho chủ thể dữ liệu cá nhân lý do cần gia hạn và chịu trách nhiệm chứng minh việc gia hạn là cần thiết, hợp lý.

5. Khi nhận được yêu cầu thực hiện các biện pháp, giải pháp bảo vệ dữ liệu cá nhân của mình theo đúng thủ tục của chủ thể dữ liệu cá nhân, cơ quan có thẩm quyền hoặc cơ quan, tổ chức, cá nhân liên quan đến xử lý dữ liệu cá nhân phải phản hồi trong thời hạn 02 ngày làm việc, cung cấp đầy đủ thông tin cho chủ thể dữ liệu cá nhân về thủ tục và thực hiện trong thời hạn 15 ngày.

Tùy theo tính chất, mức độ phức tạp của yêu cầu, trường hợp cần gia hạn thời gian xử lý thì kéo dài thêm tối đa 01 lần gia hạn trong thời hạn không quá 15 ngày, bên kiểm soát dữ liệu cá nhân, bên kiểm soát và xử lý dữ liệu cá nhân thông báo cho chủ thể dữ liệu cá nhân lý do cần gia hạn và chịu trách nhiệm chứng minh việc gia hạn là cần thiết, hợp lý.

Điều 6. Phương thức thể hiện sự đồng ý của chủ thể dữ liệu cá nhân

1. Các phương thức xin sự đồng ý của chủ thể dữ liệu cá nhân phải bảo đảm khả năng kiểm chứng được về việc xác định chủ thể dữ liệu cá nhân đã thực hiện sự đồng ý, thời điểm và nội dung được đồng ý, bao gồm:

- a) Bằng văn bản;
- b) Bằng cuộc gọi ghi âm;
- c) Cú pháp đồng ý qua tin nhắn điện thoại;
- d) Qua thư điện tử, trên trang thông tin điện tử, nền tảng, ứng dụng có thiết lập kỹ thuật xin sự đồng ý;

đ) Bằng các phương thức khác phù hợp có thể in, sao chép bằng văn bản, bao gồm cả dưới dạng điện tử hoặc định dạng kiểm chứng được.

2. Bên kiểm soát dữ liệu, bên kiểm soát và xử lý dữ liệu cá nhân phải lưu trữ sự đồng ý của chủ thể dữ liệu. Trong trường hợp có tranh chấp, trách nhiệm chứng minh sự đồng ý của chủ thể dữ liệu thuộc về bên kiểm soát dữ liệu cá nhân, bên kiểm soát và xử lý dữ liệu cá nhân.

3. Bên kiểm soát dữ liệu cá nhân, bên kiểm soát và xử lý dữ liệu cá nhân không được thiết lập phương thức mặc định đồng ý hoặc tạo ra các chỉ dẫn không rõ ràng, gây hiểu lầm giữa đồng ý và không đồng ý cho chủ thể dữ liệu. Các thiết lập mặc định sẵn có phải đảm bảo nguyên tắc bảo vệ dữ liệu cá nhân, tôn trọng các quyền của chủ thể dữ liệu cá nhân.

4. Đối với việc xin sự đồng ý xử lý dữ liệu cá nhân nhạy cảm, chủ thể dữ liệu phải được thông báo rằng dữ liệu cần xử lý là dữ liệu cá nhân nhạy cảm.

Điều 7. Chuyển giao dữ liệu cá nhân

1. Tổ chức, cá nhân chuyển giao dữ liệu cá nhân theo điểm a, điểm c, điểm d khoản 1 Điều 17 của Luật Bảo vệ dữ liệu cá nhân phải xác lập thỏa thuận về việc chuyển giao dữ liệu cá nhân với bên nhận dữ liệu cá nhân, trong đó nêu rõ các nội dung sau:

- a) Mục đích chuyển giao dữ liệu cá nhân;
- b) Đối tượng chủ thể dữ liệu cá nhân và loại dữ liệu cá nhân được chuyển giao phù hợp với mục đích chuyển giao;
- c) Thời hạn xử lý dữ liệu cá nhân, yêu cầu về xóa, hủy dữ liệu cá nhân sau khi hoàn thành mục đích chuyển giao;
- d) Cơ sở pháp lý của việc chuyển giao dữ liệu cá nhân;
- đ) Trách nhiệm bảo vệ dữ liệu cá nhân trong quá trình chuyển giao, xử lý dữ liệu cá nhân;
- e) Trách nhiệm thực hiện các quyền của chủ thể dữ liệu cá nhân;

g) Trách nhiệm phối hợp và tuân thủ của các bên trong trường hợp phát hiện vi phạm quy định bảo vệ dữ liệu cá nhân.

2. Việc chuyển giao dữ liệu cá nhân nhạy cảm phải có biện pháp bảo mật vật lý đối với thiết bị lưu trữ và truyền tải, biện pháp mã hóa, ẩn danh dữ liệu cá nhân và các biện pháp bảo mật khác trong quá trình chuyển giao.

3. Trường hợp chuyển giao dữ liệu cá nhân theo điểm a, điểm d khoản 1 Điều 17 của Luật Bảo vệ dữ liệu cá nhân có thu phí để cung cấp dịch vụ cho chủ thể dữ liệu cá nhân hoặc để phục vụ lợi ích hợp pháp của chủ thể dữ liệu cá nhân, tổ chức, cá nhân tuân thủ các quy định như sau:

a) Phải thiết lập hệ thống kỹ thuật, cơ chế minh bạch để chủ thể dữ liệu cá nhân đồng ý chính xác, rõ ràng theo từng lần chuyển giao, trên cơ sở được biết chính xác mục đích chuyển giao, tổ chức, cá nhân tiếp nhận và xử lý dữ liệu cá nhân;

b) Chỉ được xử lý dữ liệu cá nhân đúng cho mục đích chuyển giao được chủ thể dữ liệu cá nhân đồng ý, phù hợp với ngành, nghề đăng ký kinh doanh;

c) Loại dữ liệu cá nhân chuyển giao phải giới hạn trong phạm vi mục đích chuyển giao;

d) Không được thu thập, lưu trữ, hình thành kho dữ liệu cá nhân từ hoạt động chuyển giao dữ liệu cá nhân để sử dụng cho các mục đích khác ngoài các mục đích đã được chủ thể dữ liệu cá nhân đồng ý;

đ) Xác định rõ vai trò bên kiểm soát dữ liệu cá nhân, bên xử lý dữ liệu cá nhân, bên thứ ba trong hoạt động chuyển giao dữ liệu cá nhân;

e) Phải có thỏa thuận chuyển giao, xử lý dữ liệu cá nhân trước khi chuyển và cam kết trách nhiệm, nghĩa vụ với chủ thể dữ liệu cá nhân.

4. Trường hợp chia sẻ dữ liệu cá nhân giữa các bộ phận trong cùng một cơ quan, tổ chức để xử lý dữ liệu cá nhân phù hợp với mục đích xử lý đã xác lập, cơ quan, tổ chức phải xây dựng quy trình kiểm soát việc chia sẻ, sử dụng dữ liệu cá nhân đúng quy định; có biện pháp phòng, chống việc nhân sự nội bộ cơ quan, tổ chức chia sẻ trái phép dữ liệu cá nhân với bên thứ ba.

5. Dữ liệu cá nhân phải được khử nhận dạng trước khi giao dịch trên sàn dữ liệu.

6. Cơ quan, tổ chức, cá nhân thực hiện cung cấp dữ liệu cá nhân theo khoản 2 Điều 15 của Luật Bảo vệ dữ liệu cá nhân dựa trên từng yêu cầu cụ thể của chủ thể dữ liệu thì không được coi là chuyển giao dữ liệu và không phải thực hiện theo quy định tại Điều này.

Điều 8. Bảo vệ dữ liệu cá nhân trong hoạt động tài chính, ngân hàng, hoạt động thông tin tín dụng

1. Tổ chức, cá nhân hoạt động trong lĩnh vực tài chính, ngân hàng, hoạt động thông tin tín dụng có trách nhiệm áp dụng tiêu chuẩn, quy chuẩn kỹ thuật bảo vệ dữ liệu cá nhân; quy chuẩn kỹ thuật khử nhận dạng dữ liệu cá nhân, ẩn danh dữ liệu cá nhân được ban hành và áp dụng tại Việt Nam; thực hiện đánh giá tuân thủ các quy định về bảo vệ dữ liệu cá nhân định kỳ 01 năm/lần; ghi lại nhật ký toàn bộ hoạt động xử lý dữ liệu cá nhân.

2. Tổ chức, cá nhân hoạt động trong lĩnh vực tài chính, ngân hàng, hoạt động thông tin tín dụng là bên kiểm soát dữ liệu cá nhân, bên kiểm soát và xử lý dữ liệu cá nhân khi xin sự đồng ý của chủ thể dữ liệu cá nhân phải đảm bảo nêu rõ:

a) Các mục đích xử lý dữ liệu cá nhân, bao gồm hoạt động chấm điểm, xếp hạng tín dụng, đánh giá thông tin tín dụng, đánh giá mức độ tín nhiệm về tín dụng nếu có;

b) Nguồn thu thập dữ liệu cá nhân và các bên thu thập, chia sẻ dữ liệu cá nhân liên quan;

c) Thời gian lưu trữ dữ liệu cá nhân;

d) Cơ chế, cách thức rút lại sự đồng ý và chính sách xóa, hủy dữ liệu cá nhân theo quy định.

3. Trong thời hạn không quá 72 giờ sau khi phát hiện lộ, mất dữ liệu nhạy cảm của chủ thể dữ liệu cá nhân trong lĩnh vực tài chính, ngân hàng, hoạt động thông tin tín dụng, tổ chức, cá nhân trực tiếp thu thập dữ liệu cá nhân của chủ thể dữ liệu có trách nhiệm thông báo cho cơ quan chuyên trách bảo vệ dữ liệu

cá nhân và chủ thể dữ liệu cá nhân. Nội dung thông báo cần đảm bảo tối thiểu các nội dung quy định tại khoản 1 Điều 28 Nghị định này.

Điều 9. Bảo vệ dữ liệu cá nhân trong xử lý dữ liệu lớn

1. Xử lý dữ liệu lớn có chứa dữ liệu cá nhân là hoạt động xử lý dữ liệu cá nhân ở quy mô lớn, có tính liên tục, tích hợp từ nhiều nguồn khác nhau, có khả năng phân tích hành vi, dự đoán xu hướng hoặc phân loại người dùng.

2. Trường hợp xử lý dữ liệu lớn có chứa dữ liệu cá nhân, cơ quan, tổ chức, cá nhân có liên quan có trách nhiệm:

a) Tuân thủ các quy định về bảo vệ dữ liệu cá nhân trong quá trình xử lý dữ liệu ngay từ thời điểm bắt đầu xử lý;

b) Chỉ thu thập, xử lý và lưu trữ dữ liệu cá nhân đúng phạm vi, phù hợp với mục đích cụ thể, rõ ràng;

c) Xây dựng chính sách lưu trữ, xóa, hủy dữ liệu cá nhân phù hợp, đúng quy định pháp luật;

d) Tổ chức đào tạo, phổ biến và nâng cao nhận thức về bảo mật dữ liệu cá nhân và các biện pháp bảo vệ dữ liệu cá nhân cho nhân viên định kỳ, đặc biệt là nhân sự trực tiếp xử lý dữ liệu cá nhân. Tăng cường nhận thức về tầm quan trọng của bảo vệ dữ liệu cá nhân trong tổ chức;

đ) Có thỏa thuận với bên thứ ba, đối tác và nhà cung cấp dịch vụ đảm bảo tuân thủ đầy đủ các quy định về bảo vệ dữ liệu cá nhân;

e) Có cơ chế thông báo và giải thích phù hợp cho chủ thể dữ liệu về việc dữ liệu cá nhân của họ được sử dụng trong hệ thống phân tích dữ liệu lớn.

3. Cơ quan, tổ chức, cá nhân áp dụng các biện pháp bảo vệ dữ liệu cá nhân trong quá trình xử lý dữ liệu lớn, bao gồm:

a) Áp dụng các biện pháp bảo đảm an ninh mạng, bảo mật dữ liệu, phòng chống thất thoát dữ liệu cá nhân trong quá trình lưu trữ, xử lý, truyền tải dữ liệu cá nhân;

b) Sử dụng phương thức xác thực mạnh, yêu cầu tối thiểu xác thực đa yếu tố (mật khẩu, mã PIN kết hợp với mật khẩu dùng một lần, thiết bị ký số hoặc yếu tố sinh trắc học), phù hợp với mức độ nhạy cảm của dữ liệu cá nhân; phân

quyền truy cập để đảm bảo chỉ những người có quyền mới có thể truy cập dữ liệu cá nhân;

c) Thực hiện mã hóa, ẩn danh dữ liệu cá nhân (quá trình tách các dữ liệu xác định một con người cụ thể để lưu trữ và bảo mật riêng biệt, các dữ liệu cá nhân sau quá trình này được sử dụng để xử lý mà không thể xác định một con người cụ thể) trong quá trình chuyển giao, cung cấp dữ liệu cá nhân, trừ trường hợp pháp luật chuyên ngành có quy định khác hoặc khi việc xử lý yêu cầu dữ liệu ở dạng bản rõ để phục vụ phòng, chống tội phạm, phòng chống rửa tiền, bảo đảm an ninh quốc gia, xử lý khiếu nại, tranh chấp của khách hàng. Trong các trường hợp này, cơ quan, tổ chức phải áp dụng bổ sung các giải pháp bảo mật để bảo đảm dữ liệu cá nhân không bị truy cập, sử dụng trái phép;

d) Thực hiện giám sát liên tục, sử dụng các công cụ giám sát để theo dõi hoạt động truy cập dữ liệu cá nhân và phát hiện các hành vi bất thường;

đ) Thực hiện kiểm tra, đánh giá định kỳ về an ninh mạng và bảo mật dữ liệu để phát hiện, ngăn chặn và khắc phục lỗ hổng bảo mật.

Điều 10. Bảo vệ dữ liệu cá nhân trong hệ thống trí tuệ nhân tạo, vũ trụ ảo

1. Các tổ chức, cá nhân được quyền sử dụng dữ liệu cá nhân để nghiên cứu, phát triển các thuật toán tự học, hệ thống trí tuệ nhân tạo và các hệ thống tự động khác nhưng cần bảo đảm tuân thủ các quy định về bảo vệ dữ liệu cá nhân.

2. Dữ liệu từ kết quả suy luận của trí tuệ nhân tạo nếu có thể được sử dụng để xác định hoặc giúp xác định một con người cụ thể thì phải được áp dụng các biện pháp bảo vệ dữ liệu cá nhân theo quy định của pháp luật.

3. Bên kiểm soát dữ liệu cá nhân, bên kiểm soát và xử lý dữ liệu cá nhân có trách nhiệm thông báo cho chủ thể dữ liệu về việc xử lý dữ liệu cá nhân tự động, giải thích nguyên tắc hoạt động của thuật toán và ảnh hưởng đối với quyền và lợi ích hợp pháp của chủ thể dữ liệu; đưa ra các lựa chọn để chủ thể dữ liệu có quyền không tham gia.

4. Vũ trụ ảo (metaverse) là một vũ trụ kỹ thuật số kết hợp các khía cạnh của truyền thông xã hội, trò chơi trực tuyến, thực tế tăng cường (AR), thực tế ảo (VR), Internet và điện tử để cho phép người dùng sử dụng công nghệ thực tế ảo để tương tác.

5. Các tổ chức, cá nhân áp dụng các biện pháp bảo vệ dữ liệu cá nhân trong hệ thống trí tuệ nhân tạo, vũ trụ ảo, gồm:

a) Nghiên cứu, xây dựng và triển khai hệ thống đáp ứng các tiêu chuẩn an ninh mạng, tiêu chuẩn bảo vệ dữ liệu toàn diện cho các hệ thống trí tuệ nhân tạo, đặc biệt chú trọng các yếu tố: bảo mật thông tin, độ tin cậy của thuật toán, tính ổn định hệ thống và khả năng phòng chống tấn công mạng;

b) Thiết lập cơ chế giám sát hoạt động của hệ thống trí tuệ nhân tạo trên hai phương diện: giám sát của cơ quan nhà nước có thẩm quyền; trách nhiệm giải trình đối với chủ thể dữ liệu cá nhân của bên kiểm soát dữ liệu cá nhân, bên kiểm soát và xử lý dữ liệu cá nhân.

c) Xây dựng cơ chế bảo vệ dữ liệu cá nhân theo tiêu chuẩn phù hợp, phát triển hệ thống giám sát và cảnh báo sớm các nguy cơ an ninh mạng;

d) Thiết lập cơ chế kiểm soát, ngăn chặn việc lợi dụng trí tuệ nhân tạo, vũ trụ ảo vào các hoạt động xâm phạm an ninh quốc gia, trật tự an toàn xã hội;

đ) Thực hiện đánh giá tuân thủ các quy định về bảo vệ dữ liệu cá nhân định kỳ 01 năm/lần.

6. Chủ thể dữ liệu cá nhân phải có quyền chỉnh sửa, ẩn danh, xóa hồ sơ nhận dạng, kể cả khi nền tảng lưu trữ lịch sử hành vi.

Điều 11. Bảo vệ dữ liệu cá nhân trong công nghệ chuỗi khối

1. Các cơ quan, tổ chức, cá nhân có liên quan khi xử lý dữ liệu cá nhân trong công nghệ chuỗi khối có trách nhiệm tuân thủ các quy định về bảo vệ dữ liệu cá nhân ngay trong quá trình nghiên cứu, phát triển các sản phẩm, dịch vụ, ứng dụng, hệ thống sử dụng công nghệ chuỗi khối và trong quá trình xử lý dữ liệu cá nhân.

2. Cơ quan, tổ chức, cá nhân áp dụng các biện pháp bảo vệ dữ liệu cá nhân khi xử lý dữ liệu cá nhân trong công nghệ chuỗi khối, bao gồm:

a) Chỉ áp dụng các thuật toán mã hóa, thuật toán băm, thuật toán ký số đảm bảo an toàn;

b) Không lưu trữ trực tiếp dữ liệu cá nhân trên chuỗi khối, chỉ lưu trữ khi dữ liệu cá nhân đã được khử nhận dạng hoặc lưu trữ giá trị băm của dữ liệu cá nhân;

c) Thực hiện đánh giá tuân thủ các quy định về bảo vệ dữ liệu cá nhân định kỳ 01 năm/lần.

Điều 12. Bảo vệ dữ liệu cá nhân trong điện toán đám mây

1. Các cơ quan, tổ chức, cá nhân có liên quan phải áp dụng các biện pháp kỹ thuật và tổ chức để ngăn chặn dữ liệu cá nhân bị truy cập trái phép khi triển khai dịch vụ điện toán đám mây.

2. Các tổ chức, cá nhân ký kết hợp đồng có liên quan tới xử lý dữ liệu cá nhân với các tổ chức cung cấp dịch vụ điện toán đám mây có trách nhiệm như sau:

a) Nêu rõ trong nội dung hợp đồng về việc chấp hành quy định của pháp luật Việt Nam về bảo vệ dữ liệu cá nhân; cung cấp thông tin về bộ phận, nhân sự bảo vệ dữ liệu cá nhân; chấp hành quy định về thủ tục hành chính liên quan tới bảo vệ dữ liệu cá nhân theo quy định của pháp luật;

b) Xác định rõ luồng xử lý dữ liệu cá nhân, vai trò các bên trong hoạt động cung cấp dịch vụ điện toán đám mây và trách nhiệm tương ứng;

c) Có yêu cầu về các biện pháp bảo mật, kỹ thuật, tổ chức và được nêu rõ trong hợp đồng;

d) Thông báo ngay lập tức cho các bên liên quan bất kỳ sự thay đổi nào có thể ảnh hưởng tới dữ liệu cá nhân;

đ) Tuân thủ thời hạn xử lý dữ liệu cá nhân, yêu cầu về xóa, hủy dữ liệu cá nhân;

e) Bảo đảm thực hiện các quyền của chủ thể dữ liệu cá nhân;

g) Thực hiện đầy đủ các biện pháp kỹ thuật để bảo đảm quyền truy cập dữ liệu cá nhân được phân cấp một cách hợp lý.

3. Các tổ chức cung cấp dịch vụ điện toán đám mây:

a) Chấp hành các quy định về bảo vệ dữ liệu cá nhân của Việt Nam, cung cấp thông tin về bộ phận, nhân sự bảo vệ dữ liệu cá nhân, chấp hành quy định về thủ tục hành chính liên quan tới bảo vệ dữ liệu cá nhân theo quy định của pháp luật;

b) Đề nghị các nhà thầu phụ thực hiện các quy định và nghĩa vụ bảo vệ dữ liệu cá nhân theo quy định của pháp luật;

c) Áp dụng các biện pháp kỹ thuật và tổ chức ở mức phù hợp với quy mô, mức độ xử lý dữ liệu cá nhân của mình;

d) Thực hiện đánh giá tuân thủ các quy định về bảo vệ dữ liệu cá nhân định kỳ 01 năm/lần.

4. Dữ liệu cá nhân trên điện toán đám mây phải được mã hoá ở trạng thái nghỉ và truyền, kèm theo phân quyền truy cập nghiêm ngặt.

Điều 13. Điều kiện của nhân sự bảo vệ dữ liệu cá nhân, bộ phận bảo vệ dữ liệu cá nhân trong cơ quan, tổ chức

1. Việc chỉ định nhân sự bảo vệ dữ liệu cá nhân hoặc bộ phận bảo vệ dữ liệu cá nhân phải được thực hiện bằng văn bản chính thức của cơ quan, tổ chức đó; thể hiện việc phân công, chức năng nhiệm vụ, quyền hạn và các yêu cầu khác đối với công tác bảo vệ dữ liệu cá nhân trong cơ quan, tổ chức đó.

2. Nhân sự bảo vệ dữ liệu cá nhân được cơ quan, tổ chức chỉ định phải đáp ứng đủ các điều kiện năng lực như sau:

- a) Có trình độ cao đẳng trở lên;
- b) Có ít nhất 02 năm kinh nghiệm công tác (kể từ thời điểm tốt nghiệp) liên quan đến một trong các lĩnh vực về pháp chế, công nghệ thông tin, an ninh mạng, an ninh dữ liệu, quản trị rủi ro, kiểm soát tuân thủ, quản lý nhân sự, tổ chức cán bộ;
- c) Đã được đào tạo, bồi dưỡng kiến thức pháp luật và kỹ năng chuyên môn về bảo vệ dữ liệu cá nhân.

3. Trường hợp cơ quan, tổ chức thành lập bộ phận bảo vệ dữ liệu cá nhân, các nhân sự trong bộ phận phải đáp ứng đủ các điều kiện năng lực quy định tại khoản 2 Điều này.

4. Cơ quan, tổ chức chịu trách nhiệm đánh giá, lựa chọn nhân sự bảo vệ dữ liệu cá nhân.

5. Cơ quan, tổ chức ký thỏa thuận trách nhiệm bảo mật với nhân sự bảo vệ dữ liệu cá nhân, có thể thỏa thuận về các trường hợp miễn trừ trách nhiệm khi xảy ra vi phạm hoặc thiệt hại đối với dữ liệu cá nhân được bảo vệ.

6. Cơ quan, tổ chức chỉ định nhân sự bảo vệ dữ liệu cá nhân hoặc bộ phận bảo vệ dữ liệu cá nhân có trách nhiệm đào tạo, bồi dưỡng kiến thức, kỹ năng về bảo vệ dữ liệu cá nhân cho nhân sự bảo vệ dữ liệu cá nhân.

Điều 14. Nhiệm vụ của bộ phận bảo vệ dữ liệu cá nhân, nhân sự bảo vệ dữ liệu cá nhân trong cơ quan, tổ chức

1. Bộ phận bảo vệ dữ liệu cá nhân có chức năng, nhiệm vụ như sau:

a) Tổ chức xây dựng chính sách, quy trình, quy định, biểu mẫu để tuân thủ các quy định pháp luật về bảo vệ dữ liệu cá nhân;

b) Tổ chức triển khai thực hiện các quyền của chủ thể dữ liệu cá nhân;

c) Định kỳ tổ chức đánh giá thực trạng tuân thủ pháp luật về bảo vệ dữ liệu cá nhân của tổ chức bằng báo cáo đánh giá mức độ thực hiện các nghĩa vụ theo quy định pháp luật để đề xuất các biện pháp nâng cao hiệu quả tuân thủ pháp luật, phòng ngừa và kiểm soát rủi ro trong hoạt động xử lý dữ liệu cá nhân;

d) Thực hiện lập hồ sơ đánh giá tác động chuyển dữ liệu cá nhân xuyên biên giới, hồ sơ đánh giá tác động xử lý dữ liệu cá nhân, tiếp nhận và báo cáo vi phạm về bảo vệ dữ liệu cá nhân và thực hiện các yêu cầu khác của cơ quan có thẩm quyền theo quy định;

đ) Xây dựng kế hoạch và triển khai đào tạo, bồi dưỡng định kỳ về bảo vệ dữ liệu cá nhân trong cơ quan, tổ chức;

e) Tổ chức triển khai thực hiện các biện pháp kỹ thuật bảo mật dữ liệu cá nhân, tiêu chuẩn, quy chuẩn bảo vệ dữ liệu cá nhân, kế hoạch ứng cứu khẩn cấp sự cố bảo vệ dữ liệu cá nhân;

g) Nghiên cứu và đề xuất các quyết định liên quan đến bảo vệ dữ liệu cá nhân.

2. Nhân sự bảo vệ dữ liệu cá nhân có nhiệm vụ như sau:

a) Tham mưu xây dựng chính sách, quy trình, quy định, biểu mẫu để tuân thủ các quy định pháp luật về bảo vệ dữ liệu cá nhân;

b) Tham gia triển khai thực hiện các quyền của chủ thể dữ liệu cá nhân;

c) Tham gia hoạt động định kỳ đánh giá thực trạng tuân thủ pháp luật về bảo vệ dữ liệu cá nhân và đề xuất các biện pháp nâng cao hiệu quả tuân thủ pháp luật, phòng ngừa và kiểm soát rủi ro;

d) Thực hiện lập hồ sơ đánh giá tác động chuyển dữ liệu cá nhân xuyên biên giới, hồ sơ đánh giá tác động xử lý dữ liệu cá nhân, tiếp nhận và báo cáo

vi phạm về bảo vệ dữ liệu cá nhân và thực hiện các yêu cầu khác của cơ quan có thẩm quyền theo quy định;

đ) Tham gia các chương trình, khóa học bồi dưỡng về bảo vệ dữ liệu cá nhân;

e) Tham gia thực hiện các biện pháp kỹ thuật bảo mật dữ liệu cá nhân, tiêu chuẩn, quy chuẩn bảo vệ dữ liệu cá nhân, kế hoạch ứng cứu khẩn cấp sự cố bảo vệ dữ liệu cá nhân.

Điều 15. Cá nhân cung cấp dịch vụ bảo vệ dữ liệu cá nhân

1. Cá nhân cung cấp dịch vụ bảo vệ dữ liệu cá nhân là người đáp ứng đủ các điều kiện năng lực quy định tại khoản 2 Điều này, được cơ quan, tổ chức thuê làm nhân sự bảo vệ dữ liệu cá nhân.

2. Cá nhân cung cấp dịch vụ bảo vệ dữ liệu cá nhân phải đáp ứng đủ các điều kiện năng lực như sau:

a) Có trình độ cao đẳng trở lên;

b) Có ít nhất 03 năm kinh nghiệm công tác (kể từ thời điểm tốt nghiệp) liên quan đến một trong các lĩnh vực về pháp chế, xử lý dữ liệu cá nhân, an ninh mạng, an ninh dữ liệu, quản trị rủi ro, kiểm soát tuân thủ;

c) Đã được đào tạo, bồi dưỡng chuyên sâu kiến thức pháp luật và kỹ năng chuyên môn về bảo vệ dữ liệu cá nhân.

3. Cơ quan, tổ chức có nhu cầu thuê cá nhân cung cấp dịch vụ bảo vệ dữ liệu cá nhân tiến hành xem xét điều kiện năng lực theo khoản 2 Điều này, giao kết hợp đồng sử dụng nhân sự bảo vệ dữ liệu cá nhân; công khai thông tin về nhân sự bảo vệ dữ liệu cá nhân cho chủ thể dữ liệu cá nhân và các bên liên quan được biết.

4. Cá nhân cung cấp dịch vụ bảo vệ dữ liệu cá nhân có trách nhiệm:

a) Thực hiện dịch vụ theo đúng phạm vi và nhiệm vụ trong hợp đồng, thỏa thuận;

b) Không lợi dụng việc cung cấp dịch vụ để thực hiện các hành vi vi phạm pháp luật;

c) Thực hiện xóa, hủy dữ liệu cá nhân xử lý trong quá trình cung cấp dịch vụ sau khi đã hoàn thành hợp đồng và theo quy định pháp luật.

Điều 16. Tổ chức cung cấp dịch vụ bảo vệ dữ liệu cá nhân

1. Tổ chức cung cấp dịch vụ bảo vệ dữ liệu cá nhân:

a) Là tổ chức, doanh nghiệp có chức năng, nhiệm vụ hoặc ngành nghề, lĩnh vực kinh doanh về công nghệ, pháp lý hoặc tư vấn về công nghệ, pháp lý được cơ quan, tổ chức thuê để tư vấn việc tuân thủ quy định bảo vệ dữ liệu cá nhân và thực hiện nhiệm vụ bảo vệ dữ liệu cá nhân theo thỏa thuận;

b) Có tối thiểu 03 nhân sự đáp ứng đủ các điều kiện năng lực theo khoản 2 Điều 15 Nghị định này;

c) Đã cung cấp các sản phẩm, dịch vụ liên quan đến bảo mật, an ninh mạng, công nghệ thông tin, đánh giá tiêu chuẩn, tư vấn về bảo vệ dữ liệu cá nhân.

2. Tổ chức cung cấp dịch vụ bảo vệ dữ liệu cá nhân phải xây dựng hồ sơ năng lực chứng minh khả năng bảo vệ dữ liệu cá nhân và cung cấp cho cơ quan, tổ chức có nhu cầu sử dụng dịch vụ. Hồ sơ phải thể hiện ngành nghề, lĩnh vực kinh doanh; quy mô, phạm vi, kinh nghiệm cung cấp dịch vụ; chính sách cung cấp dịch vụ; tiêu chuẩn, trình độ, năng lực nhân sự; các văn bản, giấy tờ minh chứng có liên quan.

3. Cơ quan, tổ chức có nhu cầu thuê dịch vụ bảo vệ dữ liệu cá nhân tiến hành xem xét hồ sơ năng lực, giao kết hợp đồng sử dụng dịch vụ và thỏa thuận xử lý dữ liệu cá nhân với tổ chức bảo vệ dữ liệu cá nhân; công khai thông tin về tổ chức bảo vệ dữ liệu cá nhân đó cho chủ thể dữ liệu cá nhân và các bên liên quan được biết.

4. Cơ quan, tổ chức tùy theo nhu cầu có thể đồng thời chỉ định nhân sự bảo vệ dữ liệu cá nhân, bộ phận bảo vệ dữ liệu cá nhân và thuê cá nhân, tổ chức cung cấp dịch vụ bảo vệ dữ liệu cá nhân.

5. Căn cứ vào thỏa thuận với cơ quan, tổ chức thuê dịch vụ bảo vệ dữ liệu cá nhân, tổ chức cung cấp dịch vụ bảo vệ dữ liệu cá nhân thực hiện các nhiệm vụ của bộ phận bảo vệ dữ liệu cá nhân cho cơ quan, tổ chức đó.

6. Tổ chức cung cấp dịch vụ bảo vệ dữ liệu cá nhân có trách nhiệm:

- a) Thực hiện dịch vụ theo đúng phạm vi và nhiệm vụ trong hợp đồng, thỏa thuận;
- b) Không lợi dụng việc cung cấp dịch vụ để thực hiện các hành vi vi phạm pháp luật;
- c) Thực hiện xóa, hủy dữ liệu cá nhân xử lý trong quá trình cung cấp dịch vụ sau khi đã hoàn thành hợp đồng và theo quy định pháp luật.

Chương III

HỒ SƠ, TRÌNH TỰ, THỦ TỤC VỀ DỮ LIỆU CÁ NHÂN

Điều 17. Chuyển dữ liệu cá nhân xuyên biên giới

1. Bên kiểm soát dữ liệu cá nhân, bên kiểm soát và xử lý dữ liệu cá nhân, Bên Xử lý dữ liệu cá nhân và Bên thứ ba thực hiện hoạt động chuyển dữ liệu cá nhân xuyên biên giới trong các trường hợp sau đây:

- a) Hoạt động lưu trữ dữ liệu cá nhân có sự chuyển giao dữ liệu cá nhân thu thập, lưu trữ tại Việt Nam đến hệ thống máy chủ đặt ngoài lãnh thổ nước Cộng hòa xã hội chủ nghĩa Việt Nam hoặc trên dịch vụ điện toán đám mây của nhà cung cấp dịch vụ ở nước ngoài;
- b) Hoạt động chuyển dữ liệu cá nhân từ cơ quan, tổ chức, cá nhân từ Việt Nam cho bên nhận là tổ chức, cá nhân ở nước ngoài;
- c) Hoạt động xử lý dữ liệu cá nhân được thu thập tại Việt Nam và chuyển đến nền tảng ở ngoài lãnh thổ nước Cộng hòa xã hội chủ nghĩa Việt Nam để tiếp tục xử lý.

2. Cơ quan chuyên trách bảo vệ dữ liệu cá nhân quyết định yêu cầu bên chuyển dữ liệu xuyên biên giới ngừng chuyển dữ liệu cá nhân xuyên biên giới trong trường hợp:

- a) Khi phát hiện dữ liệu cá nhân được chuyển được sử dụng vào hoạt động xâm phạm quốc phòng, an ninh quốc gia;
- b) Có hành vi vi phạm các quy định về bảo vệ dữ liệu cá nhân có thể gây tổn hại đến quốc phòng, an ninh quốc gia.

3. Các trường hợp khác ngoài các trường hợp theo quy định tại điểm a, b, c khoản 6 Điều 20 Luật Bảo vệ dữ liệu cá nhân không phải thực hiện quy định về đánh giá tác động chuyển dữ liệu cá nhân xuyên biên giới bao gồm:

- a) Hoạt động báo chí, truyền thông theo quy định của pháp luật;
- b) Việc chuyển dữ liệu cá nhân xuyên biên giới đã được công khai theo quy định của pháp luật;
- c) Trong các tình huống khẩn cấp, thực sự cần thiết phải cung cấp dữ liệu cá nhân xuyên biên giới để bảo vệ tính mạng, sức khỏe và an toàn tài sản của cá nhân; để thực hiện nhiệm vụ, nghĩa vụ theo quy định của pháp luật;
- d) Hoạt động 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 của pháp luật;
- đ) Việc 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.

Điều 18. Điều kiện, trình tự, thủ tục, thành phần hồ sơ đánh giá tác động chuyển dữ liệu cá nhân xuyên biên giới

1. Cơ quan, tổ chức, cá nhân có hoạt động chuyển dữ liệu cá nhân xuyên biên giới theo quy định tại khoản 1 Điều 20 Luật Bảo vệ dữ liệu cá nhân phải lập hồ sơ đánh giá tác động chuyển dữ liệu cá nhân xuyên biên giới theo quy định tại Điều này.

2. Hồ sơ đánh giá tác động chuyển dữ liệu cá nhân xuyên biên giới bao gồm:

- a) Báo cáo đánh giá tác động chuyển dữ liệu cá nhân xuyên biên giới theo Mẫu số 09 tại Phụ lục của Nghị định này;
- b) Bản sao hợp đồng hoặc văn bản chuyển giao dữ liệu cá nhân thể hiện sự ràng buộc, trách nhiệm giữa các tổ chức, cá nhân chuyển và nhận dữ liệu cá nhân xuyên biên giới;
- c) Chính sách, quy trình, quy định, biểu mẫu và các tài liệu khác có liên quan về bảo vệ dữ liệu cá nhân của cơ quan, tổ chức, cá nhân có hoạt động chuyển dữ liệu cá nhân xuyên biên giới.

3. Báo cáo đánh giá tác động chuyển dữ liệu cá nhân xuyên biên giới bao gồm các nội dung:

a) Thông tin và chi tiết liên lạc của bên chuyển dữ liệu cá nhân, bên nhận dữ liệu cá nhân, bên xử lý dữ liệu cá nhân và các bên khác có liên quan đến hoạt động chuyển dữ liệu cá nhân xuyên biên giới;

b) Chi tiết liên lạc của bộ phận, nhân sự bảo vệ dữ liệu cá nhân; tổ chức, cá nhân cung cấp dịch vụ bảo vệ dữ liệu cá nhân (nếu có) của bên chuyển dữ liệu cá nhân, bên nhận dữ liệu cá nhân;

c) Mô tả và luận giải mục đích chuyển dữ liệu cá nhân xuyên biên giới, loại dữ liệu cá nhân chuyển xuyên biên giới, chi tiết các hoạt động chuyển và xử lý dữ liệu cá nhân xuyên biên giới và sơ đồ luồng xử lý dữ liệu cá nhân;

d) Mô tả và luận giải về việc thực hiện xin sự đồng ý của chủ thể dữ liệu cá nhân, chính sách lưu trữ, xóa, hủy dữ liệu cá nhân;

đ) Phương án bảo đảm an toàn dữ liệu cá nhân sau khi chuyển xuyên biên giới, các biện pháp bảo vệ dữ liệu cá nhân, tiêu chuẩn bảo vệ dữ liệu cá nhân được áp dụng;

e) Sơ đồ hệ thống, mô tả tính năng của hệ thống lưu trữ, xử lý dữ liệu cá nhân sau khi tiếp nhận dữ liệu cá nhân xuyên biên giới;

g) Quy trình về việc bên tiếp nhận dữ liệu cá nhân xuyên biên giới chuyển giao, cung cấp dữ liệu cá nhân cho bên thứ ba;

h) Kết quả tự đánh giá tuân thủ quy định về bảo vệ dữ liệu cá nhân của cơ quan, tổ chức, cá nhân có hoạt động chuyển dữ liệu cá nhân xuyên biên giới;

i) Đánh giá mức độ bảo vệ dữ liệu cá nhân của bên nhận dữ liệu cá nhân; mức độ ảnh hưởng, rủi ro của việc chuyển và xử lý dữ liệu cá nhân xuyên biên giới; hậu quả, thiệt hại không mong muốn có khả năng xảy ra, các biện pháp giảm thiểu hoặc loại bỏ nguy cơ, rủi ro đó.

4. Hồ sơ đánh giá tác động chuyển dữ liệu cá nhân xuyên biên giới phải luôn có sẵn để phục vụ hoạt động kiểm tra, đánh giá của cơ quan chuyên trách bảo vệ dữ liệu cá nhân.

Bên chuyển dữ liệu cá nhân xuyên biên giới nộp 01 bản chính hồ sơ đầy đủ bằng phương thức trực tuyến hoặc trực tiếp hoặc qua dịch vụ bưu chính về cơ quan chuyên trách bảo vệ dữ liệu cá nhân kèm theo Mẫu số 01a/01b tại Phụ lục của Nghị định này trong thời hạn 60 ngày kể từ ngày tiến hành chuyển dữ liệu cá nhân xuyên biên giới.

5. Cơ quan chuyên trách bảo vệ dữ liệu cá nhân đánh giá và trả kết quả đối với Hồ sơ đánh giá tác động chuyển dữ liệu cá nhân xuyên biên giới đạt yêu cầu hoặc không đạt yêu cầu trong thời hạn 15 ngày.

6. Cơ quan chuyên trách bảo vệ dữ liệu cá nhân đánh giá, yêu cầu bên chuyển dữ liệu cá nhân xuyên biên giới hoàn thiện Hồ sơ đánh giá tác động chuyển dữ liệu cá nhân xuyên biên giới trong thời hạn 30 ngày đối với trường hợp hồ sơ chưa đầy đủ và đúng quy định. Trường hợp bên chuyển dữ liệu cá nhân không thực hiện hoàn thiện hồ sơ theo đúng quy định, cơ quan chuyên trách bảo vệ dữ liệu cá nhân xem xét áp dụng các quy định về xử phạt vi phạm hành chính trong lĩnh vực bảo vệ dữ liệu cá nhân.

7. Bên chuyển dữ liệu cá nhân xuyên biên giới cập nhật, bổ sung Hồ sơ đánh giá tác động chuyển dữ liệu cá nhân xuyên biên giới theo quy định của Điều 20 Nghị định này.

Điều 19. Điều kiện, trình tự, thủ tục, thành phần hồ sơ đánh giá tác động xử lý dữ liệu cá nhân

1. Bên kiểm soát dữ liệu cá nhân, bên kiểm soát và xử lý dữ liệu cá nhân, bên xử lý dữ liệu cá nhân lập và lưu giữ Hồ sơ đánh giá tác động xử lý dữ liệu cá nhân của mình kể từ thời điểm bắt đầu xử lý dữ liệu cá nhân.

2. Hồ sơ đánh giá tác động xử lý dữ liệu cá nhân của bên kiểm soát dữ liệu cá nhân, bên kiểm soát và xử lý dữ liệu cá nhân, bên xử lý dữ liệu cá nhân bao gồm:

a) Báo cáo đánh giá tác động xử lý dữ liệu cá nhân theo Mẫu số 10 tại Phụ lục của Nghị định này;

b) Bản sao hợp đồng hoặc thỏa thuận về việc xử lý dữ liệu cá nhân, thể hiện sự ràng buộc, trách nhiệm giữa các tổ chức, cá nhân trong hoạt động xử lý dữ liệu cá nhân;

c) Chính sách, quy trình, quy định, biểu mẫu và các tài liệu khác có liên quan về bảo vệ dữ liệu cá nhân của bên kiểm soát dữ liệu cá nhân, bên kiểm soát và xử lý dữ liệu cá nhân, bên xử lý dữ liệu cá nhân.

3. Báo cáo đánh giá tác động xử lý dữ liệu cá nhân bao gồm các nội dung:

a) Thông tin và chi tiết liên lạc của bên kiểm soát dữ liệu cá nhân, bên kiểm soát và xử lý dữ liệu cá nhân, bên xử lý dữ liệu cá nhân, bên thứ ba;

b) Chi tiết liên lạc của bộ phận, nhân sự bảo vệ dữ liệu cá nhân; tổ chức, cá nhân cung cấp dịch vụ bảo vệ dữ liệu cá nhân (nếu có) của bên kiểm soát dữ liệu cá nhân, bên kiểm soát và xử lý dữ liệu cá nhân, bên xử lý dữ liệu cá nhân, bên thứ ba;

c) Mô tả và luận giải mục đích xử lý dữ liệu cá nhân, loại dữ liệu cá nhân xử lý, chi tiết các hoạt động xử lý dữ liệu cá nhân và sơ đồ luồng dữ liệu cá nhân;

d) Mô tả và luận giải về việc thực hiện xin sự đồng ý của chủ thể dữ liệu cá nhân, chính sách lưu trữ, xóa, hủy dữ liệu cá nhân;

đ) Phương án bảo đảm an toàn dữ liệu cá nhân, các biện pháp bảo vệ dữ liệu cá nhân, sơ đồ thiết kế hệ thống, tiêu chuẩn bảo vệ dữ liệu cá nhân được áp dụng;

e) Kết quả đánh giá tuân thủ quy định về bảo vệ dữ liệu cá nhân;

g) Đánh giá mức độ ảnh hưởng, rủi ro của hoạt động xử lý dữ liệu cá nhân; hậu quả, thiệt hại không mong muốn có khả năng xảy ra, các biện pháp giảm thiểu hoặc loại bỏ nguy cơ, rủi ro đó.

4. Hồ sơ đánh giá tác động xử lý dữ liệu cá nhân phải luôn có sẵn để phục vụ hoạt động kiểm tra, đánh giá của Cơ quan chuyên trách bảo vệ dữ liệu cá nhân và nộp 01 bản chính bằng phương thức trực tuyến hoặc trực tiếp hoặc qua dịch vụ bưu chính về cơ quan chuyên trách bảo vệ dữ liệu cá nhân kèm theo Mẫu số 02a/02b tại Phụ lục của Nghị định này trong thời hạn 60 ngày kể từ ngày tiến hành xử lý dữ liệu cá nhân.

5. Cơ quan chuyên trách bảo vệ dữ liệu cá nhân đánh giá và trả kết quả đối với Hồ sơ đánh giá tác động xử lý dữ liệu cá nhân đạt yêu cầu hoặc không đạt yêu cầu trong thời hạn 15 ngày.

6. Cơ quan chuyên trách bảo vệ dữ liệu cá nhân đánh giá, yêu cầu bên kiểm soát dữ liệu cá nhân, bên kiểm soát và xử lý dữ liệu cá nhân, bên xử lý dữ liệu cá nhân hoàn thiện Hồ sơ đánh giá tác động xử lý dữ liệu cá nhân trong thời hạn 30 ngày đối với trường hợp hồ sơ chưa đầy đủ và đúng quy định. Trường hợp bên kiểm soát dữ liệu cá nhân, bên kiểm soát và xử lý dữ liệu cá nhân, bên xử lý dữ liệu cá nhân không thực hiện hoàn thiện hồ sơ theo đúng quy định, cơ quan chuyên trách bảo vệ dữ liệu cá nhân xem xét áp dụng các quy định về xử phạt vi phạm hành chính trong lĩnh vực bảo vệ dữ liệu cá nhân.

7. Bên kiểm soát dữ liệu cá nhân, bên kiểm soát và xử lý dữ liệu cá nhân, bên xử lý dữ liệu cá nhân cập nhật, bổ sung Hồ sơ đánh giá tác động xử lý dữ liệu cá nhân theo quy định của Điều 20 Nghị định này.

Điều 20. Cập nhật hồ sơ đánh giá tác động xử lý dữ liệu cá nhân và hồ sơ đánh giá tác động chuyển dữ liệu cá nhân xuyên biên giới

1. Hồ sơ chuyển dữ liệu cá nhân xuyên biên giới và hồ sơ đánh giá tác động xử lý dữ liệu cá nhân được cập nhật định kỳ 06 tháng kể từ lần đầu nộp hồ sơ trong các trường hợp sau:

a) Khi phát sinh mục đích chuyển dữ liệu cá nhân mới, mục đích xử lý dữ liệu cá nhân mới;

b) Khi phát sinh hoặc thay đổi bên kiểm soát dữ liệu cá nhân, bên kiểm soát và xử lý dữ liệu cá nhân, bên xử lý dữ liệu cá nhân, bên thứ ba.

2. Các trường hợp thay đổi cần cập nhật ngay trong thời hạn 10 ngày bao gồm:

a) Khi cơ quan, tổ chức, đơn vị được tổ chức lại, chấm dứt hoạt động, giải thể, phá sản theo quy định của pháp luật;

b) Khi có sự thay đổi thông tin về tổ chức, cá nhân cung cấp dịch vụ bảo vệ dữ liệu cá nhân;

c) Khi phát sinh hoặc thay đổi ngành, nghề, dịch vụ kinh doanh liên quan đến xử lý dữ liệu cá nhân đã đăng ký trong hồ sơ đánh giá tác động xử lý dữ liệu cá nhân, hồ sơ đánh giá tác động chuyển dữ liệu cá nhân xuyên biên giới.

3. Việc cập nhật hồ sơ đánh giá tác động xử lý dữ liệu cá nhân và hồ sơ đánh giá tác động chuyển dữ liệu cá nhân xuyên biên giới được thực hiện theo Mẫu số 03a/03b tại Phụ lục của Nghị định này, nộp bằng phương thức trực tuyến hoặc trực tiếp hoặc qua dịch vụ bưu chính về cơ quan chuyên trách bảo vệ dữ liệu cá nhân.

Điều 21. Dịch vụ xử lý dữ liệu cá nhân

1. 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.

2. Dịch vụ chấm điểm, xếp hạng, đánh giá mức độ tín nhiệm của chủ thể dữ liệu cá nhân.

3. Dịch vụ thu thập, xử lý dữ liệu cá nhân trực tuyến từ trang web, ứng dụng, phần mềm và mạng xã hội.

4. 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.

5. 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.

6. 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.

7. Dịch vụ mã hóa dữ liệu cá nhân trong quá trình truyền tải và lưu trữ.

8. 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.

9. Dịch vụ nền tảng ứng dụng cung cấp dữ liệu vị trí cá nhân.

Điều 22. Điều kiện của tổ chức kinh doanh dịch vụ xử lý dữ liệu cá nhân

1. Là tổ chức, doanh nghiệp được thành lập và hoạt động theo pháp luật Việt Nam, đáp ứng các điều kiện quy định tại Điều này.

2. Điều kiện về nhân sự:

a) Người đứng đầu phụ trách chuyên môn về xử lý dữ liệu cá nhân của tổ chức là công dân Việt Nam, thường trú tại Việt Nam;

b) Có đội ngũ quản lý, điều hành đáp ứng được yêu cầu chuyên môn xử lý dữ liệu cá nhân;

c) Có tối thiểu 03 nhân sự đủ điều kiện năng lực theo quy định tại khoản 2 Điều 13 Nghị định này.

3. Có hạ tầng, hệ thống trang thiết bị, cơ sở vật chất và công nghệ phù hợp với dịch vụ xử lý dữ liệu cá nhân.

4. Có kết quả đạt yêu cầu đối với hồ sơ đánh giá tác động xử lý dữ liệu cá nhân và hồ sơ đánh giá tác động chuyển dữ liệu cá nhân xuyên biên giới trong trường hợp có chuyển dữ liệu cá nhân xuyên biên giới.

Điều 23. Trách nhiệm của tổ chức kinh doanh dịch vụ xử lý dữ liệu cá nhân

1. Tuân thủ đầy đủ các quy định pháp luật về bảo vệ dữ liệu cá nhân; trách nhiệm, nghĩa vụ của bên kiểm soát và xử lý dữ liệu cá nhân, bên xử lý dữ liệu cá nhân.

2. Xây dựng khung quản trị rủi ro về bảo vệ dữ liệu cá nhân phù hợp với dịch vụ cung cấp.

3. Thực hiện đánh giá hiện trạng tuân thủ và mức độ tín nhiệm về bảo vệ dữ liệu cá nhân định kỳ 01 năm/lần.

4. Áp dụng tiêu chuẩn, quy chuẩn liên quan đến an ninh dữ liệu, bảo vệ dữ liệu cá nhân, an ninh mạng.

5. Xây dựng quy định về trách nhiệm và quyền hạn của tổ chức trong xử lý dữ liệu cá nhân.

6. Bảo đảm xử lý dữ liệu cá nhân đúng mục đích, giới hạn việc thu thập, chuyển giao, lưu trữ phù hợp và theo quy định pháp luật; ngăn chặn truy cập, thu thập, sử dụng, tiết lộ trái phép hoặc các rủi ro tương tự trong hoạt động xử lý dữ liệu cá nhân.

7. Trường hợp là bên xử lý dữ liệu cá nhân, tổ chức yêu cầu bên kiểm soát dữ liệu cá nhân xin sự đồng ý của chủ thể dữ liệu theo quy định trước khi cung cấp dịch vụ, bảo đảm chủ thể dữ liệu cá nhân được biết về loại dữ liệu cá nhân xử lý, mục đích xử lý và tổ chức cung cấp dịch vụ xử lý dữ liệu cá nhân.

8. Tổ chức kinh doanh dịch vụ xử lý dữ liệu cá nhân thực hiện việc xác thực danh tính tổ chức theo quy định pháp luật về định danh và xác thực điện tử.

Điều 24. Thẩm quyền cấp, cấp lại, cấp đổi, thu hồi Giấy chứng nhận đủ điều kiện kinh doanh dịch vụ xử lý dữ liệu cá nhân

1. Bộ Công an cấp, cấp lại, cấp đổi, thu hồi Giấy chứng nhận đủ điều kiện cung cấp dịch vụ xử lý dữ liệu cá nhân.

2. Bộ trưởng Bộ Công an giao trách nhiệm cho cơ quan chuyên trách bảo vệ dữ liệu cá nhân thực hiện việc cấp, cấp lại, cấp đổi, thu hồi Giấy chứng nhận đủ điều kiện cung cấp dịch vụ xử lý dữ liệu cá nhân theo quy định.

Điều 25. Hồ sơ, trình tự, thủ tục về việc cấp Chứng nhận đủ điều kiện kinh doanh dịch vụ xử lý dữ liệu cá nhân

1. Hồ sơ đề nghị cấp Chứng nhận đủ điều kiện kinh doanh dịch vụ xử lý dữ liệu cá nhân, gồm:

a) Đơn đề nghị cấp Chứng nhận đủ điều kiện kinh doanh dịch vụ xử lý dữ liệu cá nhân theo Mẫu số 04 tại Phụ lục của Nghị định này;

b) Bản sao Giấy chứng nhận đăng ký doanh nghiệp;

c) Văn bản chỉ định bộ phận bảo vệ dữ liệu cá nhân hoặc hợp đồng sử dụng dịch vụ bảo vệ dữ liệu cá nhân theo quy định;

d) Đề án đề nghị cấp Giấy chứng nhận đủ điều kiện kinh doanh dịch vụ xử lý dữ liệu cá nhân;

đ) Bảng cấp và các giấy tờ chứng minh khác của nhân sự quy định tại điểm c khoản 2 Điều 22 Nghị định này;

e) Tổ chức không phải nộp giấy tờ quy định tại điểm b khoản này trong trường hợp cơ quan nhà nước khai thác được trên cơ sở dữ liệu.

2. Đề án đề nghị cấp Giấy chứng nhận đủ điều kiện kinh doanh dịch vụ xử lý dữ liệu cá nhân bao gồm các nội dung:

a) Sự cần thiết, mục tiêu;

b) Nội dung, lĩnh vực đề nghị phê duyệt;

c) Ngành nghề, lĩnh vực kinh doanh, phương án kinh doanh;

d) Quy mô hoạt động xử lý dữ liệu cá nhân dự kiến;

đ) Khung quản trị rủi ro về bảo vệ dữ liệu cá nhân;

e) Kế hoạch đánh giá hiện trạng tuân thủ và mức độ tín nhiệm về bảo vệ dữ liệu cá nhân định kỳ;