

TÀI LIỆU QUẢN TRIỆT NỘI DUNG CƠ BẢN CỦA LUẬT BẢO VỆ DỮ LIỆU CÁ NHÂN

I. GIỚI THIỆU CHUNG VỀ LUẬT BẢO VỆ DỮ LIỆU CÁ NHÂN

1. Sự cần thiết ban hành

Ngày 26/6/2025, tại kỳ họp thứ 9, Quốc hội khóa XV đã thông qua Luật Bảo vệ dữ liệu cá nhân số 91/2025/QH15 và có hiệu lực thi hành kể từ ngày 01/01/2026. Luật số 91/2025/QH15 thể chế hóa quan điểm chỉ đạo của Đảng về bảo vệ quyền con người, quyền công dân, quyền và lợi ích hợp pháp của cá nhân; tạo sự đồng bộ, thống nhất, xuyên suốt của hệ thống pháp luật, phục vụ cuộc cách mạng đột phá phát triển khoa học công nghệ, đổi mới sáng tạo và chuyển đổi số quốc gia theo tinh thần Nghị quyết 57-NQ/TW của Bộ Chính trị; góp phần bảo đảm an ninh con người, chủ quyền dữ liệu trong kỷ nguyên mới của dân tộc.

2. Mục tiêu

Việc xây dựng Luật Bảo vệ dữ liệu cá nhân nhằm hoàn thiện, thống nhất hệ thống pháp luật về bảo vệ dữ liệu cá nhân, tạo hành lang pháp lý cho công tác bảo vệ dữ liệu cá nhân, nâng cao năng lực bảo vệ dữ liệu cá nhân cho các tổ chức, cá nhân trong nước tiếp cận trình độ quốc tế, khu vực; đẩy mạnh sử dụng dữ liệu cá nhân đúng pháp luật phục vụ phát triển kinh tế, xã hội.

3. Quan điểm

Một là, cụ thể hóa tinh thần của Hiến pháp năm 2013, thể chế hóa chủ trương, chính sách của Đảng, Nhà nước về công nhận, tôn trọng, bảo vệ dữ liệu cá nhân, bảo đảm quyền con người, quyền cơ bản của công dân. Xác định dữ liệu cá nhân là nguồn tài nguyên quan trọng cần được bảo vệ, sử dụng phục vụ phát triển kinh tế, xã hội và bảo đảm quyền con người, quyền công dân, bảo vệ Tổ quốc.

Hai là, đáp ứng tốt yêu cầu phát triển kinh tế - xã hội, bảo đảm quốc phòng - an ninh; thúc đẩy ứng dụng, phát huy tối đa các thành tựu khoa học và công nghệ; xác định lộ trình phù hợp thực hiện công tác bảo vệ dữ liệu cá nhân phù hợp với thực tiễn nước ta hiện nay.

Ba là, phù hợp với các quy định của pháp luật, rà soát, tạo nền tảng để xây dựng một hệ thống pháp luật hoàn chỉnh, đồng bộ về bảo vệ dữ liệu cá nhân; hài hòa với pháp luật quốc tế, bảo đảm sự phù hợp với các quy định, cam kết quốc tế mà Việt Nam tham gia ký kết hoặc là thành viên.

4. Bố cục

Luật số 91/2025/QH15 gồm 05 Chương, 39 Điều, quy định về dữ liệu cá nhân, bảo vệ dữ liệu cá nhân và quyền, nghĩa vụ, trách nhiệm của cơ quan, tổ chức, cá nhân có liên quan; trong đó:

- Chương I gồm 08 điều, quy định các vấn đề chung, như: phạm vi điều chỉnh, đối tượng áp dụng, nguyên tắc bảo vệ dữ liệu cá nhân, quyền và nghĩa vụ của chủ thể dữ liệu cá nhân, hành vi bị nghiêm cấm, xử lý vi phạm pháp luật về bảo vệ dữ liệu cá nhân.

- Chương II gồm 24 điều, quy định về bảo vệ dữ liệu cá nhân trong quá trình xử lý dữ liệu và bảo vệ dữ liệu cá nhân trong một số hoạt động, lĩnh vực cụ thể.

- Chương III gồm 03 điều, quy định về lực lượng bảo vệ dữ liệu cá nhân, điều kiện bảo đảm bảo vệ dữ liệu cá nhân.

- Chương IV gồm 02 điều, quy định trách nhiệm của cơ quan, tổ chức, cá nhân về bảo vệ dữ liệu cá nhân.

- Chương V gồm 02 điều, quy định hiệu lực thi hành, điều khoản chuyển tiếp.

II. NHỮNG NỘI DUNG CƠ BẢN TRONG LUẬT BẢO VỆ DỮ LIỆU CÁ NHÂN

Chương I

NHỮNG QUY ĐỊNH CHUNG

1. Phạm vi điều chỉnh, việc áp dụng pháp luật, đối tượng áp dụng

Phạm vi điều chỉnh của Luật theo Điều 1 là về dữ liệu cá nhân, bảo vệ dữ liệu cá nhân và quyền, nghĩa vụ, trách nhiệm của cơ quan, tổ chức, cá nhân có liên quan. Có thể hiểu đây là luật gốc, thống nhất các quy định về dữ liệu cá nhân và bảo vệ dữ liệu cá nhân. Do đó, Điều 5 đã quy định về việc áp dụng pháp luật về bảo vệ dữ liệu cá nhân, như sau:

- Hoạt động bảo vệ dữ liệu cá nhân trên lãnh thổ nước Cộng hòa xã hội chủ nghĩa Việt Nam thực hiện theo quy định của Luật này và quy định khác của pháp luật có liên quan.

- Các luật, nghị quyết của Quốc hội ban hành trước ngày Luật này có hiệu lực thi hành được áp dụng quy định cụ thể về bảo vệ dữ liệu cá nhân trong luật, nghị quyết đó với điều kiện không trái với nguyên tắc bảo vệ dữ liệu cá nhân theo quy định của Luật này.

- Các luật, nghị quyết của Quốc hội ban hành sau ngày Luật này có hiệu lực thi hành có quy định về bảo vệ dữ liệu cá nhân khác với quy định của Luật này thì phải quy định cụ thể nội dung thực hiện hoặc không thực hiện theo quy định của Luật này, nội dung thực hiện theo quy định của luật, nghị quyết đó.

- Để tránh chồng chéo giữa Luật này và Luật Dữ liệu, cắt giảm tối đa thủ tục hành chính và chi phí tuân thủ cho doanh nghiệp, Luật này quy định trường hợp cơ quan, tổ chức, cá nhân thực hiện việc đánh giá tác động xử lý dữ liệu cá nhân, đánh giá tác động chuyển dữ liệu cá nhân xuyên biên giới thì không phải thực hiện đánh giá rủi ro xử lý dữ liệu cá nhân, đánh giá tác động chuyển dữ liệu cá nhân xuyên biên giới theo quy định của pháp luật về dữ liệu.

Luật này áp dụng đối với cả cơ quan, tổ chức, cá nhân Việt Nam và nước ngoài, cụ thể:

(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.

2. Giải thích từ ngữ

Luật đã xây dựng và thống nhất một số khái niệm quan trọng trong lĩnh vực bảo vệ dữ liệu cá nhân, như: khái niệm dữ liệu cá nhân bao trùm cả môi trường truyền thống và môi trường số; bảo vệ dữ liệu cá nhân; xử lý dữ liệu cá nhân; khử nhận dạng dữ liệu cá nhân; làm rõ khái niệm và nội hàm của dữ liệu cá nhân cơ bản, dữ liệu cá nhân nhạy cảm; chủ thể dữ liệu cá nhân và các bên liên quan trong quá trình xử lý dữ liệu cá nhân. Cụ thể:

- *Dữ liệu cá nhân* là dữ liệu số hoặc thông tin dưới dạng khác xác định hoặc giúp xác định một con người cụ thể, bao gồm: dữ liệu cá nhân cơ bản và dữ liệu cá nhân nhạy cảm.

Khái niệm này đã bao quát hơn so với Nghị định số 13/2023/NĐ-CP, mở rộng điều chỉnh cả dữ liệu cá nhân ở dạng truyền thống (trong văn bản, tài liệu, hồ sơ...) và trên môi trường điện tử (dữ liệu số). Khoản 1 Điều 3 Luật Dữ liệu đã quy định về *Dữ liệu số* là dữ liệu về sự vật, hiện tượng, sự kiện, bao gồm một hoặc kết hợp các dạng âm thanh, hình ảnh, chữ số, chữ viết, ký hiệu được thể hiện dưới dạng kỹ thuật số. Điều kiện để những dữ liệu này trở thành dữ liệu cá nhân chính là việc “xác định” một con người cụ thể (có thể hiểu là định danh con người đó) hoặc các dữ liệu, thông tin khi kết hợp lại với nhau thì “giúp xác định” một con người cụ thể.

Vậy trong trường hợp nào dữ liệu cá nhân không còn là dữ liệu cá nhân nữa? Luật đã quy định khái niệm *Khử nhận dạng dữ liệu cá nhân* là quá trình thay đổi hoặc xóa thông tin để tạo ra dữ liệu mới không thể xác định hoặc không thể giúp xác định được một con người cụ thể. Dữ liệu cá nhân sau khi khử nhận dạng không còn là dữ liệu cá nhân. Như vậy, khử nhận dạng dữ liệu cá nhân có thể hiểu là quá trình khử đi các thông tin, dữ liệu giúp định danh một con người cụ thể để tạo ra kết quả cuối cùng không còn là dữ liệu cá nhân.

Điều 14 quy định cụ thể về trách nhiệm của cơ quan, tổ chức, cá nhân khi khử nhận dạng phải kiểm soát và giám sát chặt chẽ quá trình khử nhận dạng dữ liệu cá nhân; ngăn chặn việc truy cập trái phép, sao chép, chiếm đoạt, làm lộ, làm mất dữ liệu cá nhân trong quá trình khử nhận dạng. Đặc biệt, việc khử nhận dạng phải đảm bảo tạo ra kết quả cuối cùng không còn là dữ liệu cá nhân và sau đó không tái nhận dạng dữ liệu đó.

Khác với khử nhận dạng dữ liệu cá nhân, Điều 12 quy định mã hóa dữ liệu cá nhân là việc chuyển đổi dữ liệu cá nhân sang dạng không nhận biết được dữ liệu cá nhân nếu không được giải mã. Mã hóa được hiểu là một biện pháp để bảo

vệ dữ liệu cá nhân; dữ liệu cá nhân sau khi được mã hóa vẫn là dữ liệu cá nhân bởi luôn có khả năng giải mã dữ liệu đó trở về dạng ban đầu khi chưa mã hóa.

- *Dữ liệu cá nhân cơ bản* là dữ liệu cá nhân phản ánh các yếu tố nhân thân, lai lịch phổ biến, thường xuyên sử dụng trong các giao dịch, quan hệ xã hội, thuộc danh mục do Chính phủ ban hành.

Ví dụ như: họ và tên, ngày tháng năm sinh, số điện thoại, dân tộc, giới tính...

Dữ liệu cá nhân nhạy cảm là dữ liệu cá nhân gắn liền với quyền riêng tư của cá nhân, khi bị xâm phạm sẽ gây ảnh hưởng trực tiếp đến quyền, lợi ích hợp pháp của cơ quan, tổ chức, cá nhân, thuộc danh mục do Chính phủ ban hành.

Ví dụ như: đặc điểm sinh trắc học, xu hướng tính dục, thông tin tài chính tín dụng, thông tin sức khỏe, dữ liệu vị trí...

Như vậy, sự khác biệt căn bản giữa dữ liệu cá nhân cơ bản và dữ liệu cá nhân nhạy cảm là tính chất phản ánh sự riêng tư và mức độ ảnh hưởng, hậu quả, thiệt hại có thể xảy ra khi dữ liệu cá nhân đó bị xâm phạm. Danh mục chi tiết sẽ do Chính phủ ban hành tại Nghị định hướng dẫn Luật.

- *Bảo vệ dữ liệu cá nhân* là việc cơ quan, tổ chức, cá nhân sử dụng lực lượng, phương tiện, biện pháp để phòng, chống hoạt động xâm phạm dữ liệu cá nhân.

Đây cũng là mục tiêu của việc ban hành Luật này, đó là phòng, chống hoạt động xâm phạm dữ liệu cá nhân, bảo vệ quyền riêng tư, quyền con người trong bối cảnh thực trạng xâm phạm dữ liệu cá nhân diễn ra tràn lan, phổ biến như hiện nay.

- *Chủ thể dữ liệu cá nhân* là người được dữ liệu cá nhân phản ánh.

Khái niệm này được hình thành để xác lập các quyền và nghĩa vụ của mỗi cá nhân cung cấp dữ liệu cá nhân của mình cho các bên liên quan.

- *Xử lý dữ liệu cá nhân* là hoạt động tác động đến dữ liệu cá nhân, bao gồm một hoặc nhiều hoạt động như sau: thu thập, phân tích, tổng hợp, mã hóa, giải mã, chỉnh sửa, xóa, hủy, khử nhận dạng, cung cấp, công khai, chuyển giao dữ liệu cá nhân và hoạt động khác tác động đến dữ liệu cá nhân.

Có thể hiểu hoạt động xử lý dữ liệu cá nhân khá rộng, là mọi hoạt động sử dụng đến dữ liệu cá nhân đó. Trên thực tế, các hoạt động này thường hình thành nên một chuỗi các hoạt động liên quan, như thu thập, lưu trữ, chuyển giao..., từ đó tạo nên các luồng dữ liệu cá nhân. Do đó, để kiểm soát luồng dữ liệu cá nhân từ điểm bắt đầu đến các điểm sử dụng tiếp theo, Luật hình thành nên 04 bên đóng các vai trò khác nhau trên cơ sở mục đích và phương tiện xử lý để tuân thủ các trách nhiệm, nghĩa vụ với chủ thể dữ liệu cá nhân. Cụ thể:

- Các bên liên quan trong hoạt động xử lý dữ liệu cá nhân:

+ *Bên kiểm soát dữ liệu cá nhân* là cơ quan, tổ chức, cá nhân quyết định mục đích và phương tiện xử lý dữ liệu cá nhân.

+ *Bên xử lý dữ liệu cá nhân* là cơ quan, tổ chức, cá nhân thực hiện việc xử lý dữ liệu cá nhân theo yêu cầu của bên kiểm soát dữ liệu cá nhân hoặc bên kiểm soát và xử lý dữ liệu cá nhân thông qua hợp đồng.

+ *Bên kiểm soát và xử lý dữ liệu cá nhân* là cơ quan, tổ chức, cá nhân quyết định mục đích, phương tiện và trực tiếp xử lý dữ liệu cá nhân.

+ *Bên thứ ba* là tổ chức, cá nhân ngoài chủ thể dữ liệu cá nhân, bên kiểm soát dữ liệu cá nhân, bên kiểm soát và xử lý dữ liệu cá nhân, bên xử lý dữ liệu cá nhân tham gia vào việc xử lý dữ liệu cá nhân theo quy định của pháp luật.

3. Nguyên tắc bảo vệ dữ liệu cá nhân

Luật đưa ra 06 nguyên tắc bảo vệ dữ liệu cá nhân, trong đó có 03 nguyên tắc quan trọng trong quá trình xử lý dữ liệu cá nhân, đó là:

- Chỉ được thu thập, xử lý dữ liệu cá nhân đúng phạm vi, mục đích cụ thể, rõ ràng, bảo đảm tuân thủ quy định của pháp luật.

- Bảo đảm tính chính xác của dữ liệu cá nhân và được chỉnh sửa, cập nhật, bổ sung khi cần thiết; được lưu trữ trong khoảng thời gian phù hợp với mục đích xử lý dữ liệu cá nhân, trừ trường hợp pháp luật có quy định khác.

- Thực hiện đồng bộ có hiệu quả các biện pháp, giải pháp về thể chế, kỹ thuật, con người phù hợp để bảo vệ dữ liệu cá nhân.

Ngoài ra là các nguyên tắc tuân thủ; phòng, chống vi phạm pháp luật về bảo vệ dữ liệu cá nhân; bảo vệ dữ liệu cá nhân gắn với bảo vệ lợi ích quốc gia, dân tộc, phục vụ phát triển kinh tế - xã hội, bảo đảm quốc phòng, an ninh và đối ngoại; bảo đảm hài hòa giữa bảo vệ dữ liệu cá nhân với bảo vệ quyền, lợi ích hợp pháp của cơ quan, tổ chức, cá nhân.

4. Quyền và nghĩa vụ của chủ thể dữ liệu cá nhân

Các quyền của chủ thể dữ liệu cá nhân được quy định kế thừa Nghị định số 13/2023/NĐ-CP để xác lập, công nhận các quyền của cá nhân đối với thông tin, dữ liệu của mình, phù hợp với thông lệ quốc tế và là nền tảng để thực hiện các cơ chế bảo vệ chủ thể dữ liệu cá nhân.

06 quyền của chủ thể dữ liệu cá nhân bao gồm:

(1) Được biết về hoạt động xử lý dữ liệu cá nhân;

(2) Đồng ý hoặc không đồng ý, yêu cầu rút lại sự đồng ý cho phép xử lý dữ liệu cá nhân;

(3) Xem, chỉnh sửa hoặc yêu cầu chỉnh sửa dữ liệu cá nhân;

(4) Yêu cầu cung cấp, xóa, hạn chế xử lý dữ liệu cá nhân; gửi yêu cầu phản đối xử lý dữ liệu cá nhân;

(5) Khiếu nại, tố cáo, khởi kiện, yêu cầu bồi thường thiệt hại theo quy định của pháp luật;

(6) Yêu cầu cơ quan có thẩm quyền hoặc cơ quan, tổ chức, cá nhân liên quan đến xử lý dữ liệu cá nhân thực hiện các biện pháp, giải pháp bảo vệ dữ liệu cá nhân của mình theo quy định của pháp luật.

Bên cạnh quyền, Luật có quy định mới về nghĩa vụ của chủ thể dữ liệu cá nhân để đảm bảo tính cân bằng, tăng cường trách nhiệm của tất cả các bên liên quan đến dữ liệu cá nhân, trong đó có chủ thể dữ liệu cá nhân, bao gồm:

- a) Tự bảo vệ dữ liệu cá nhân của mình;
- b) Tôn trọng, bảo vệ dữ liệu cá nhân của người khác;
- c) Cung cấp đầy đủ, chính xác dữ liệu cá nhân của mình theo quy định của pháp luật, theo hợp đồng hoặc khi đồng ý cho phép xử lý dữ liệu cá nhân của mình;
- d) Chấp hành pháp luật về bảo vệ dữ liệu cá nhân và tham gia phòng, chống hoạt động xâm phạm dữ liệu cá nhân.

5. Hành vi bị nghiêm cấm và xử lý vi phạm pháp luật về bảo vệ dữ liệu cá nhân

Trong bối cảnh chuyển đổi số diễn ra sâu rộng trên hầu hết các lĩnh vực, dữ liệu cá nhân được chuyển lên môi trường điện tử thường xuyên, liên tục dẫn đến tình trạng lộ, mất dữ liệu cá nhân diễn ra phổ biến trong quá trình chuyển giao, lưu trữ, trao đổi phục vụ hoạt động kinh doanh hoặc do biện pháp bảo vệ không tương xứng dẫn tới bị chiếm đoạt và đăng tải công khai¹. Hoạt động mua, bán dữ liệu cá nhân diễn ra dưới nhiều hình thức, như: (1) Doanh nghiệp không có thỏa thuận xử lý dữ liệu cá nhân chặt chẽ với đối tác, để đối tác chuyển giao, bán cho các đối tác khác; (2) Chủ động thu thập, hình thành kho dữ liệu cá nhân, phân tích, xử lý các loại dữ liệu đó để tiến hành kinh doanh, buôn bán; (3) Rao bán dữ liệu cá nhân số lượng lớn, có hệ thống, có tổ chức, cam kết “bảo hành” và có khả năng cập nhật dữ liệu, trích xuất dữ liệu theo yêu cầu người mua; (4) Lập doanh nghiệp vận hành các hệ thống kỹ thuật chuyên thu thập trái phép dữ liệu cá nhân, cài ẩn trong các trang mạng để thu thập thông tin tự động, phân tích thành tệp dữ liệu cá nhân có giá trị; (5) Tấn công, xâm nhập hệ thống thông tin để chiếm đoạt dữ liệu cá nhân, tán phát mã độc thu thập dữ liệu cá nhân trên môi trường mạng.

Thực tiễn triển khai công tác bảo vệ dữ liệu cá nhân theo Nghị định số 13/2023/NĐ-CP cho thấy, nhiều tổ chức, doanh nghiệp thu thập thừa dữ liệu cá nhân so với ngành nghề, sản phẩm, dịch vụ kinh doanh, thiếu cơ sở pháp lý khi thu thập dữ liệu cá nhân, không xác định được các luồng xử lý dữ liệu. Nhiều hoạt động thu thập, xử lý dữ liệu cá nhân mà chưa có sự đồng ý của chủ thể dữ liệu, không thể lấy ý kiến về sự đồng ý đối với những dữ liệu cá nhân đã thu thập.

¹ Một số vụ việc điển hình như: việc Công ty VNG để lộ hơn 163 triệu tài khoản khách hàng; Công ty Thế giới di động và Điện máy xanh để lộ hơn 5 triệu email và hàng chục nghìn thông tin thẻ thanh toán như Visa, thẻ tín dụng của khách hàng; tin tặc đã tấn công vào hệ thống máy chủ của Việt Nam Airline, đăng tải lên Internet 411.000 tài khoản khách hàng thành viên của chương trình Bông Sen Vàng; tình trạng để lộ thông tin khách hàng để các công ty môi giới dịch vụ taxi của Việt Nam sử dụng để mời chào khách hàng qua tin nhắn SMS; dữ liệu khách hàng của Công ty FPT bị đăng tải công khai trên mạng

Để đảm bảo khả thi và ngăn chặn hiệu quả các hành vi vi phạm pháp luật về bảo vệ dữ liệu cá nhân, Luật đã quy định các hành vi bị nghiêm cấm bám sát thực tiễn, đảm bảo tính bao quát, tập trung vào những hành vi phổ biến, nghiêm trọng, bao gồm:

(1) Xử lý dữ liệu cá nhân nhằm chống lại Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam, gây ảnh hưởng đến quốc phòng, an ninh quốc gia, trật tự, an toàn xã hội, quyền, lợi ích hợp pháp của cơ quan, tổ chức, cá nhân.

(2) Cản trở hoạt động bảo vệ dữ liệu cá nhân.

(3) Lợi dụng hoạt động bảo vệ dữ liệu cá nhân để thực hiện hành vi vi phạm pháp luật.

(4) Xử lý dữ liệu cá nhân trái quy định của pháp luật.

(5) Sử dụng dữ liệu cá nhân của người khác, cho người khác sử dụng dữ liệu cá nhân của mình để thực hiện hành vi trái quy định của pháp luật.

(6) Mua, bán dữ liệu cá nhân, trừ trường hợp luật có quy định khác.

(7) Chiếm đoạt, cố ý làm lộ, làm mất dữ liệu cá nhân.

Đặc biệt, hành vi mua, bán dữ liệu cá nhân bị nghiêm cấm, trừ trường hợp luật có quy định khác sẽ tạo hành lang pháp lý để đấu tranh với tội phạm coi dữ liệu cá nhân như hàng hóa thông thường để mua, bán, xâm phạm nghiêm trọng đến quyền con người, quyền lợi hợp pháp của cá nhân, tổ chức.

Luật quy định xử lý vi phạm pháp luật về bảo vệ dữ liệu cá nhân theo hình thức xử phạt hành chính hoặc truy cứu trách nhiệm hình sự; nếu gây thiệt hại thì phải bồi thường theo quy định của pháp luật dựa trên tính chất, mức độ, hậu quả của hành vi vi phạm. Đối với hình thức xử phạt hành chính trong lĩnh vực bảo vệ dữ liệu cá nhân, áp dụng:

- Đối với hành vi mua, bán dữ liệu cá nhân: Mức phạt tiền tối đa là 10 lần khoản thu có được từ hành vi vi phạm; trường hợp không có khoản thu từ hành vi vi phạm hoặc mức phạt tính theo khoản thu có được từ hành vi vi phạm thấp hơn 03 tỷ đồng thì áp dụng mức phạt tiền tối đa là 03 tỷ đồng. Chính phủ sẽ quy định phương pháp tính khoản thu có được từ việc thực hiện hành vi vi phạm pháp luật về bảo vệ dữ liệu cá nhân.

- Đối với hành vi vi phạm quy định chuyển dữ liệu cá nhân xuyên biên giới: Mức phạt tiền tối đa là 5% doanh thu của năm trước liền kề của tổ chức đó; trường hợp không có doanh thu của năm trước liền kề hoặc mức phạt tính theo doanh thu thấp hơn 03 tỷ đồng thì áp dụng mức phạt tiền tối đa là 03 tỷ đồng.

- Đối với các hành vi vi phạm khác: Mức phạt tiền tối đa là 03 tỷ đồng với tổ chức. Mức phạt áp dụng với cá nhân bằng một phần hai mức phạt đối với tổ chức theo từng hành vi.

Chương II

BẢO VỆ DỮ LIỆU CÁ NHÂN

Qua tổng kết thi hành Nghị định số 13/2023/NĐ-CP cho thấy, việc tuân thủ các nghĩa vụ trong quá trình xử lý dữ liệu cá nhân của tổ chức, cá nhân, như: xây dựng hồ sơ đánh giá tác động xử lý dữ liệu cá nhân, đánh giá tác động chuyển dữ liệu cá nhân ra nước ngoài, thông báo vi phạm về bảo vệ dữ liệu cá nhân vẫn còn nhiều lúng túng, chậm trễ; công tác đào tạo, tập huấn về bảo vệ dữ liệu cá nhân trong các tổ chức chưa được tiến hành thường xuyên. Việc thay đổi quy trình làm việc, chính sách hiện hành của tổ chức, doanh nghiệp phù hợp với quy định về bảo vệ dữ liệu cá nhân đã được quan tâm nhưng chưa được triển khai đúng mức; việc cung cấp các giải pháp kỹ thuật bảo vệ dữ liệu cá nhân còn hạn chế, thiếu tiêu chí đánh giá các giải pháp kỹ thuật đáp ứng được yêu cầu bảo vệ dữ liệu cá nhân.

Trong khi đó, thực trạng xâm phạm dữ liệu cá nhân tiếp tục gia tăng, đặc biệt trong các lĩnh vực có quy mô xử lý dữ liệu cá nhân lớn, tính chất nhạy cảm cao, như: tài chính, ngân hàng, thông tin tín dụng, bảo hiểm, quảng cáo, mạng xã hội, trí tuệ nhân tạo, chuỗi khối... Do đó, Luật đã thiết kế Chương II gồm 02 mục: Mục 1 quy định về bảo vệ dữ liệu cá nhân trong quá trình xử lý dữ liệu (từ Điều 9 đến Điều 23) và Mục 2 quy định bảo vệ dữ liệu cá nhân trong một số hoạt động, lĩnh vực cụ thể (từ Điều 24 đến Điều 32).

Mục 1

BẢO VỆ DỮ LIỆU CÁ NHÂN

TRONG QUÁ TRÌNH XỬ LÝ DỮ LIỆU CÁ NHÂN

1. Sự đồng ý của chủ thể dữ liệu cá nhân

Quyền đồng ý là một trong những quyền quan trọng nhất, thiết lập nguyên tắc căn bản nhất cho mọi hoạt động xử lý dữ liệu cá nhân. Luật quy định tại Điều 9 về:

- Khái niệm sự đồng ý của chủ thể dữ liệu cá nhân: là việc chủ thể dữ liệu cá nhân cho phép xử lý dữ liệu cá nhân của mình, trừ trường hợp pháp luật có quy định khác.

- Điều kiện để sự đồng ý có hiệu lực (hiệu lực được tính từ thời điểm đồng ý cho đến khi chủ thể dữ liệu cá nhân thay đổi sự đồng ý đó hoặc theo quy định của pháp luật): chủ thể dữ liệu cá nhân phải tự nguyện đồng ý và trước khi đồng ý phải được biết rõ:

- a) Loại dữ liệu cá nhân được xử lý, mục đích xử lý dữ liệu cá nhân;
- b) Bên kiểm soát dữ liệu cá nhân hoặc bên kiểm soát và xử lý dữ liệu cá nhân;
- c) Các quyền, nghĩa vụ của chủ thể dữ liệu cá nhân.

- Phương thức thể hiện sự đồng ý: phải rõ ràng, cụ thể, có thể in, sao chép bằng văn bản, bao gồm cả dưới dạng điện tử hoặc định dạng kiểm chứng được.

- Nguyên tắc khi xin sự đồng ý của chủ thể dữ liệu: xin sự đồng ý với từng mục đích; không được kèm theo điều kiện bắt buộc phải đồng ý với các mục đích khác với nội dung thỏa thuận. Đặc biệt, nếu chủ thể dữ liệu cá nhân im lặng hoặc không phản hồi thì không được coi là đồng ý.

- Các trường hợp không cần xin sự đồng ý trước khi xử lý dữ liệu cá nhân: Luật quy định 04 trường hợp cụ thể và các trường hợp khác theo quy định của pháp luật, như sau:

(1) Để bảo vệ tính mạng, sức khỏe, danh dự, nhân phẩm, quyền, lợi ích hợp pháp của chủ thể dữ liệu cá nhân hoặc người khác trong trường hợp cấp bách; bảo vệ quyền hoặc lợi ích chính đáng của mình, của người khác hoặc lợi ích của Nhà nước, của cơ quan tổ chức một cách cần thiết trước hành vi xâm phạm lợi ích nói trên. Trường hợp này các bên liên quan trong hoạt động xử lý cần chứng minh được lý do không cần xin sự đồng ý.

(2) Để giải quyết tình trạng khẩn cấp; nguy cơ đe dọa an ninh quốc gia nhưng chưa đến mức ban bố tình trạng khẩn cấp; phòng, chống bạo loạn, khủng bố, phòng, chống tội phạm và vi phạm pháp luật.

(3) Phục vụ hoạt động của cơ quan nhà nước, hoạt động quản lý nhà nước theo quy định của pháp luật.

(4) Thực hiện thỏa thuận của chủ thể dữ liệu cá nhân với cơ quan, tổ chức, cá nhân có liên quan theo quy định của pháp luật.

Đặc biệt, để kiểm soát và bảo vệ chặt chẽ dữ liệu cá nhân trong các trường hợp không cần sự đồng ý của chủ thể dữ liệu cá nhân, Luật quy định thêm trách nhiệm của các bên liên quan phải thiết lập:

(1) Cơ chế giám sát thông qua: quy trình, quy định xác định rõ trách nhiệm của các bên trong quá trình xử lý dữ liệu cá nhân và định kỳ kiểm tra, đánh giá việc tuân thủ, đánh giá rủi ro; triển khai các biện pháp bảo vệ dữ liệu cá nhân phù hợp.

(2) Cơ chế tiếp nhận và xử lý phản ánh, kiến nghị từ cơ quan, tổ chức, cá nhân có liên quan.

2. Yêu cầu rút lại sự đồng ý, yêu cầu hạn chế xử lý dữ liệu cá nhân

- Sau khi chủ thể dữ liệu cá nhân đồng ý cho phép xử lý, chủ thể dữ liệu cá nhân có quyền yêu cầu rút lại sự đồng ý đó bằng cách gửi văn bản (bao gồm cả dạng điện tử hoặc định dạng kiểm chứng được) cho bên kiểm soát dữ liệu cá nhân, bên kiểm soát và xử lý dữ liệu cá nhân.

- Khi có nghi ngờ phạm vi, mục đích xử lý dữ liệu cá nhân hoặc tính chính xác của dữ liệu cá nhân, chủ thể dữ liệu cá nhân có quyền yêu cầu hạn chế xử lý dữ liệu cá nhân của mình cũng thông qua việc gửi văn bản (bao gồm cả

dạng điện tử hoặc định dạng kiểm chứng được) cho bên kiểm soát dữ liệu cá nhân, bên kiểm soát và xử lý dữ liệu cá nhân.

- Tuy nhiên, việc thực hiện yêu cầu rút lại sự đồng ý, yêu cầu hạn chế xử lý dữ liệu cá nhân không áp dụng đối với hoạt động xử lý dữ liệu cá nhân trước thời điểm chủ thể dữ liệu cá nhân yêu cầu rút lại sự đồng ý hoặc yêu cầu hạn chế xử lý dữ liệu cá nhân.

3. Thu thập, phân tích, tổng hợp dữ liệu cá nhân

- Hoạt động phân tích, tổng hợp dữ liệu cá nhân phải có sự đồng ý của chủ thể dữ liệu cá nhân trước khi thu thập, trừ trường hợp pháp luật có quy định khác. Hoạt động này có thể được thực hiện bởi Cơ quan Đảng, Nhà nước có thẩm quyền; cơ quan, tổ chức, cá nhân khác. Luật quy định về nguồn dữ liệu cá nhân được phép phân tích, tổng hợp như sau:

+ Đối với Cơ quan Đảng, Nhà nước có thẩm quyền: được phân tích, tổng hợp dữ liệu cá nhân từ nguồn dữ liệu tự thu thập hoặc được chia sẻ, cung cấp, chuyển giao, khai thác, sử dụng để phục vụ công tác lãnh đạo, chỉ đạo, quản lý nhà nước, phát triển kinh tế - xã hội theo quy định của pháp luật.

+ Đối với cơ quan, tổ chức, cá nhân khác: được phân tích, tổng hợp dữ liệu cá nhân từ nguồn dữ liệu cá nhân được phép xử lý theo quy định của pháp luật.

4. Chỉnh sửa dữ liệu cá nhân

- Trường hợp cần chỉnh sửa dữ liệu cá nhân của mình, chủ thể dữ liệu cá nhân có thể tự chỉnh sửa theo thỏa thuận hoặc đề nghị bên kiểm soát dữ liệu cá nhân, bên kiểm soát và xử lý dữ liệu cá nhân chỉnh sửa dữ liệu cá nhân của mình.

- Việc chỉnh sửa dữ liệu cá nhân phải bảo đảm tính chính xác. Trường hợp không thể chỉnh sửa dữ liệu cá nhân vì lý do chính đáng, bên kiểm soát dữ liệu cá nhân, bên kiểm soát và xử lý dữ liệu cá nhân phải thông báo để cơ quan, tổ chức, cá nhân yêu cầu biết.

5. Cung cấp dữ liệu cá nhân

- Chủ thể dữ liệu cá nhân cung cấp dữ liệu cá nhân cho cơ quan, tổ chức, cá nhân theo quy định của pháp luật (như cung cấp phục vụ hoạt động quản lý nhà nước, thực hiện các dịch vụ công...) hoặc theo thỏa thuận với cơ quan, tổ chức, cá nhân đó.

- Bên kiểm soát dữ liệu cá nhân, bên kiểm soát và xử lý dữ liệu cá nhân cung cấp dữ liệu cá nhân trong các trường hợp sau đây:

(1) Cung cấp cho chủ thể dữ liệu cá nhân theo yêu cầu của chủ thể dữ liệu cá nhân phù hợp quy định của pháp luật, thỏa thuận với chủ thể dữ liệu

(2) Cung cấp cho cơ quan, tổ chức, cá nhân khác khi được chủ thể dữ liệu cá nhân đồng ý, trừ trường hợp pháp luật có quy định khác.

- Không cung cấp dữ liệu cá nhân trong trường hợp việc cung cấp có thể gây tổn hại đến quốc phòng, an ninh quốc gia, trật tự, an toàn xã hội hoặc xâm phạm đến tính mạng, sức khỏe, tài sản của người khác.

6. Công khai dữ liệu cá nhân

- Điều kiện để công khai dữ liệu cá nhân: chỉ được công khai với mục đích cụ thể; phạm vi công khai, loại dữ liệu cá nhân được công khai phải phù hợp với mục đích công khai; không được xâm phạm đến quyền, lợi ích hợp pháp của chủ thể dữ liệu cá nhân.

- Các trường hợp được phép công khai dữ liệu cá nhân:

(1) Khi có sự đồng ý của chủ thể dữ liệu cá nhân;

(2) Thực hiện theo quy định của pháp luật;

(3) Trường hợp để giải quyết tình trạng khẩn cấp; nguy cơ đe dọa an ninh quốc gia nhưng chưa đến mức ban bố tình trạng khẩn cấp; phòng, chống bạo loạn, khủng bố, phòng, chống tội phạm và vi phạm pháp luật;

(4) Thực hiện nghĩa vụ theo hợp đồng.

- Chất lượng dữ liệu cá nhân công khai: phải bảo đảm phản ánh đúng dữ liệu cá nhân từ nguồn dữ liệu gốc và tạo thuận lợi cho cơ quan, tổ chức, cá nhân trong việc tiếp cận, khai thác, sử dụng.

- Hình thức công khai dữ liệu cá nhân, bao gồm: đăng tải dữ liệu trên trang thông tin điện tử, cổng thông tin điện tử, phương tiện thông tin đại chúng và các hình thức khác theo quy định của pháp luật.

- Trách nhiệm khi công khai dữ liệu cá nhân: Cơ quan, tổ chức, cá nhân công khai dữ liệu cá nhân phải kiểm soát và giám sát chặt chẽ việc công khai dữ liệu cá nhân để bảo đảm tuân thủ đúng mục đích, phạm vi và quy định của pháp luật; ngăn chặn việc truy cập, sử dụng, tiết lộ, sao chép, sửa đổi, xóa, hủy hoặc các hành vi xử lý trái phép khác đối với dữ liệu cá nhân đã công khai trong khả năng, điều kiện của mình.

7. Chuyển giao dữ liệu cá nhân

- Việc chuyển giao dữ liệu cá nhân được thực hiện trong 06 trường hợp:

(1) Khi có sự đồng ý của chủ thể dữ liệu cá nhân;

(2) Khi các bộ phận trong cùng một cơ quan, tổ chức chia sẻ dữ liệu cá nhân với nhau để xử lý dữ liệu cá nhân phù hợp với mục đích xử lý đã xác lập;

(3) Để tiếp tục xử lý dữ liệu cá nhân khi có sự thay đổi cơ cấu tổ chức như: trong trường hợp chia, tách, sáp nhập cơ quan, tổ chức, đơn vị hành chính và tổ chức lại, chuyển đổi hình thức sở hữu doanh nghiệp nhà nước; chia, tách, sáp nhập, hợp nhất, kết thúc hoạt động đơn vị, tổ chức; đơn vị, tổ chức được thành lập trên cơ sở kết thúc hoạt động của đơn vị, tổ chức khác;

(4) Chuyển giao giữa Bên kiểm soát dữ liệu cá nhân, bên kiểm soát và xử lý dữ liệu cá nhân với bên xử lý dữ liệu cá nhân, bên thứ ba để xử lý dữ liệu cá nhân theo quy định;

(5) Theo yêu cầu của cơ quan nhà nước có thẩm quyền;

(6) Trong các trường hợp xử lý dữ liệu cá nhân không cần sự đồng ý của chủ thể dữ liệu cá nhân tại khoản 1 Điều 19.

- 06 trường hợp chuyển giao dữ liệu cá nhân nêu trên nếu có kèm theo việc thu phí thì không được xác định là mua, bán dữ liệu cá nhân.

8. Chuyển dữ liệu cá nhân xuyên biên giới

- 03 trường hợp chuyển dữ liệu cá nhân xuyên biên giới, bao gồm:

(1) Chuyển dữ liệu cá nhân đang lưu trữ tại Việt Nam đến hệ thống lưu trữ dữ liệu đặt ngoài lãnh thổ nước Cộng hòa xã hội chủ nghĩa Việt Nam;

(2) Cơ quan, tổ chức, cá nhân tại Việt Nam chuyển dữ liệu cá nhân cho tổ chức, cá nhân ở nước ngoài;

(3) Cơ quan, tổ chức, cá nhân tại Việt Nam hoặc ở nước ngoài sử dụng nền tảng ở ngoài lãnh thổ nước Cộng hòa xã hội chủ nghĩa Việt Nam để xử lý dữ liệu cá nhân được thu thập tại Việt Nam.

- Về hồ sơ đánh giá tác động chuyển dữ liệu cá nhân xuyên biên giới:

+ Đối tượng lập hồ sơ: Cơ quan, tổ chức, cá nhân chuyển dữ liệu cá nhân xuyên biên giới, trừ 03 đối tượng sau: 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.

+ Yêu cầu: Lập, lưu giữ và gửi 01 bản chính cho cơ quan chuyên trách bảo vệ dữ liệu cá nhân trong thời gian 60 ngày kể từ ngày đầu tiên chuyển dữ liệu cá nhân xuyên biên giới.

+ Tần suất: thực hiện 01 lần cho suốt thời gian hoạt động của cơ quan, tổ chức, cá nhân đó và được cập nhật định kỳ 06 tháng khi có sự thay đổi hoặc cập nhật ngay trong các trường hợp: 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.

+ Thành phần, trình tự, thủ tục hồ sơ sẽ được Chính phủ quy định.

- Cơ quan chuyên trách bảo vệ dữ liệu cá nhân quyết định:

+ Kiểm tra chuyển dữ liệu cá nhân xuyên biên giới định kỳ không quá 01 lần trong năm hoặc kiểm tra đột xuất khi phát hiện hành vi vi phạm quy định của pháp luật về bảo vệ dữ liệu cá nhân hoặc khi xảy ra sự cố lộ, mất dữ liệu cá nhân.

+ Yêu cầu ngừng chuyển dữ liệu cá nhân xuyên biên giới của cơ quan, tổ chức, cá nhân khi phát hiện dữ liệu cá nhân được chuyển để sử dụng vào hoạt động có thể gây tổn hại đến quốc phòng, an ninh quốc gia.

- Chính phủ quy định thành phần hồ sơ, điều kiện, trình tự, thủ tục đánh giá tác động chuyển dữ liệu cá nhân xuyên biên giới.

9. Đánh giá tác động xử lý dữ liệu cá nhân

- Đối tượng lập hồ sơ: Bên kiểm soát dữ liệu cá nhân, bên kiểm soát và xử lý dữ liệu cá nhân, trừ cơ quan nhà nước có thẩm quyền không phải thực hiện quy định về đánh giá tác động xử lý dữ liệu cá nhân. Bên xử lý dữ liệu cá nhân thực hiện theo thỏa thuận với bên kiểm soát dữ liệu cá nhân, bên kiểm soát và xử lý dữ liệu cá nhân.

- Yêu cầu: lập, lưu trữ hồ sơ đánh giá tác động xử lý dữ liệu cá nhân và gửi 01 bản chính cho cơ quan chuyên trách bảo vệ dữ liệu cá nhân trong thời gian 60 ngày kể từ ngày đầu tiên xử lý dữ liệu cá nhân.

- Tần suất: thực hiện 01 lần cho suốt thời gian hoạt động của bên kiểm soát dữ liệu cá nhân, bên kiểm soát và xử lý dữ liệu cá nhân và được cập nhật trong các trường hợp tương tự như hồ sơ đánh giá tác động chuyển dữ liệu cá nhân xuyên biên giới.

- Chính phủ quy định thành phần hồ sơ, điều kiện, trình tự, thủ tục đánh giá tác động xử lý dữ liệu cá nhân.

10. Thông báo vi phạm quy định về bảo vệ dữ liệu cá nhân

- Đối tượng thực hiện thông báo: Bên kiểm soát dữ liệu cá nhân, bên kiểm soát và xử lý dữ liệu cá nhân, bên thứ ba, cơ quan, tổ chức, cá nhân.

- Trường hợp cần thông báo:

+ Khi phát hiện vi phạm quy định về bảo vệ dữ liệu cá nhân có thể gây tổn hại đến quốc phòng, an ninh quốc gia, trật tự, an toàn xã hội hoặc xâm phạm đến tính mạng, sức khỏe, danh dự, nhân phẩm, tài sản của chủ thể dữ liệu cá nhân thì phải thông báo cho cơ quan chuyên trách bảo vệ dữ liệu cá nhân chậm nhất là 72 giờ kể từ khi phát hiện hành vi vi phạm.

+ Khi bên xử lý dữ liệu cá nhân phát hiện hành vi vi phạm phải thông báo kịp thời cho bên kiểm soát dữ liệu cá nhân hoặc bên kiểm soát và xử lý dữ liệu cá nhân.

+ Các trường hợp khác cần thông báo cho cơ quan chuyên trách bảo vệ dữ liệu cá nhân: khi dữ liệu cá nhân bị xử lý sai mục đích, không đúng thỏa thuận giữa chủ thể dữ liệu cá nhân với bên kiểm soát dữ liệu cá nhân, bên kiểm soát và xử lý dữ liệu cá nhân; khi không bảo đảm quyền hoặc thực hiện không đúng quyền của chủ thể dữ liệu cá nhân; trường hợp khác theo quy định của pháp luật.

- Nội dung thông báo vi phạm: Chính phủ quy định nội dung thông báo vi phạm quy định về bảo vệ dữ liệu cá nhân.

- Yêu cầu khi phát hiện vi phạm: Bên kiểm soát dữ liệu cá nhân, bên kiểm soát và xử lý dữ liệu cá nhân phải lập biên bản xác nhận về việc xảy ra hành vi

vi phạm quy định về bảo vệ dữ liệu cá nhân, phối hợp với cơ quan chuyên trách bảo vệ dữ liệu cá nhân xử lý hành vi vi phạm.

- Trách nhiệm các bên khi phát hiện vi phạm:

+ Cơ quan chuyên trách bảo vệ dữ liệu cá nhân có trách nhiệm tiếp nhận thông báo, xử lý hành vi vi phạm quy định về bảo vệ dữ liệu cá nhân.

+ Bên kiểm soát dữ liệu cá nhân, bên kiểm soát và xử lý dữ liệu cá nhân, bên thứ ba và cơ quan, tổ chức, cá nhân có liên quan có trách nhiệm ngăn chặn hành vi vi phạm, khắc phục hậu quả xảy ra và phối hợp cơ quan chuyên trách bảo vệ dữ liệu cá nhân trong xử lý hành vi vi phạm quy định về bảo vệ dữ liệu cá nhân.

Mục 2

BẢO VỆ DỮ LIỆU CÁ NHÂN TRONG MỘT SỐ HOẠT ĐỘNG

1. Bảo vệ dữ liệu cá nhân của trẻ em, người bị mất hoặc hạn chế năng lực hành vi dân sự, người có khó khăn trong nhận thức, làm chủ hành vi

- Đối với trẻ em, người bị mất hoặc hạn chế năng lực hành vi dân sự hoặc người có khó khăn trong nhận thức, làm chủ hành vi: người đại diện theo pháp luật thay mặt thực hiện các quyền của chủ thể dữ liệu cá nhân.

- Việc xử lý dữ liệu cá nhân của trẻ em nhằm công bố, tiết lộ thông tin về đời sống riêng tư, bí mật cá nhân của trẻ em từ đủ 07 tuổi trở lên thì phải có sự đồng ý của trẻ em và người đại diện theo pháp luật.

- Ngừng xử lý dữ liệu cá nhân của trẻ em, người bị mất hoặc hạn chế năng lực hành vi dân sự, người có khó khăn trong nhận thức, làm chủ hành vi trong trường hợp sau đây:

(1) Khi rút lại sự đồng ý cho phép xử lý dữ liệu cá nhân của trẻ em, người bị mất hoặc hạn chế năng lực hành vi dân sự, người có khó khăn trong nhận thức, làm chủ hành vi, trừ trường hợp pháp luật có quy định khác;

(2) Theo yêu cầu của cơ quan có thẩm quyền khi có đủ căn cứ chứng minh việc xử lý dữ liệu cá nhân có thể xâm phạm đến quyền, lợi ích hợp pháp của trẻ em, người bị mất hoặc hạn chế năng lực hành vi dân sự, người có khó khăn trong nhận thức, làm chủ hành vi, trừ trường hợp pháp luật có quy định khác.

2. Bảo vệ dữ liệu cá nhân trong tuyển dụng, quản lý, sử dụng người lao động

- Trách nhiệm bảo vệ dữ liệu cá nhân trong quá trình tuyển dụng, bao gồm:

(1) Trách nhiệm khi thu thập dữ liệu cá nhân: Chỉ được yêu cầu cung cấp các thông tin phục vụ cho mục đích tuyển dụng của cơ quan, tổ chức, cá nhân tuyển dụng phù hợp với quy định của pháp luật; thông tin được cung cấp chỉ được sử dụng vào mục đích tuyển dụng và mục đích khác theo thỏa thuận phù hợp với quy định của pháp luật;

(2) Trách nhiệm khi xử lý dữ liệu cá nhân: Thông tin cung cấp phải được xử lý theo quy định của pháp luật và phải được sự đồng ý của người dự tuyển.

(3) Trách nhiệm nếu không tuyển dụng: Phải xóa, hủy thông tin đã cung cấp của người dự tuyển trong trường hợp không tuyển dụng, trừ trường hợp có thỏa thuận khác với người đã dự tuyển.

- Trách nhiệm bảo vệ dữ liệu cá nhân trong quản lý, sử dụng người lao động bao gồm:

(1) Trách nhiệm lưu trữ dữ liệu cá nhân của người lao động: phải lưu trữ trong thời hạn theo quy định của pháp luật hoặc theo thỏa thuận;

(2) Trách nhiệm khi chấm dứt hợp đồng lao động: Phải xóa, hủy dữ liệu cá nhân của người lao động khi chấm dứt hợp đồng, trừ trường hợp theo thỏa thuận hoặc pháp luật có quy định khác.

- Trách nhiệm khi sử dụng biện pháp công nghệ, kỹ thuật trong quản lý người lao động:

(1) Chỉ được áp dụng các biện pháp công nghệ, kỹ thuật phù hợp với quy định của pháp luật và bảo đảm quyền, lợi ích của chủ thể dữ liệu cá nhân, trên cơ sở người lao động biết rõ biện pháp đó;

(2) Không được xử lý, sử dụng dữ liệu cá nhân thu thập từ các biện pháp công nghệ, kỹ thuật trái quy định của pháp luật.

3. Bảo vệ dữ liệu cá nhân đối với thông tin sức khỏe và trong hoạt động kinh doanh bảo hiểm

- Trách nhiệm khi thu thập, xử lý thông tin sức khỏe và trong hoạt động kinh doanh bảo hiểm:

(1) Phải có sự đồng ý của chủ thể dữ liệu cá nhân trong quá trình thu thập, xử lý dữ liệu cá nhân, trừ các trường hợp không cần sự đồng ý;

(2) Áp dụng đầy đủ quy định về bảo vệ dữ liệu cá nhân, quy định khác của pháp luật có liên quan;

(3) Tuân thủ đầy đủ quy định về bảo vệ dữ liệu cá nhân khi phát triển ứng dụng về y tế, ứng dụng về kinh doanh bảo hiểm;

(4) Nêu rõ trong hợp đồng với khách hàng trường hợp kinh doanh tái bảo hiểm, nhượng tái bảo hiểm và có chuyển dữ liệu cá nhân cho đối tác.

- Trách nhiệm khi cung cấp dữ liệu cá nhân: Cơ quan, tổ chức, cá nhân hoạt động trong lĩnh vực sức khỏe không cung cấp dữ liệu cá nhân cho bên thứ ba là tổ chức cung cấp dịch vụ chăm sóc sức khỏe hoặc dịch vụ bảo hiểm sức khỏe, bảo hiểm nhân thọ, trừ trường hợp có yêu cầu bằng văn bản của chủ thể dữ liệu cá nhân hoặc trường hợp quy định tại khoản 1 Điều 19 của Luật.

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

- Trong lĩnh vực tài chính, ngân hàng, hoạt động thông tin tín dụng, tổ chức, cá nhân có trách nhiệm:

(1) Về biện pháp bảo vệ:

+ Thực hiện đầy đủ quy định về bảo vệ dữ liệu cá nhân nhạy cảm, các tiêu chuẩn an toàn, bảo mật trong hoạt động tài chính, ngân hàng theo quy định của pháp luật;

+ Áp dụng các biện pháp phòng, chống truy cập, sử dụng, tiết lộ, chỉnh sửa trái phép dữ liệu cá nhân của khách hàng; có giải pháp khôi phục dữ liệu cá nhân của khách hàng trong trường hợp bị mất; bảo mật trong quá trình thu thập, cung cấp, xử lý dữ liệu cá nhân của khách hàng phục vụ đánh giá thông tin tín dụng;

+ Thông báo cho chủ thể dữ liệu cá nhân trong trường hợp lộ, mất thông tin về tài khoản ngân hàng, tài chính, tín dụng, thông tin tín dụng.

(2) Về điều kiện khi chấm điểm, xếp hạng tín dụng, đánh giá thông tin tín dụng, đánh giá mức độ tín nhiệm về tín dụng: Chỉ được sử dụng thông tin tín dụng của chủ thể dữ liệu cá nhân để chấm điểm, xếp hạng tín dụng, đánh giá thông tin tín dụng, đánh giá mức độ tín nhiệm về tín dụng của chủ thể dữ liệu cá nhân khi có sự đồng ý của chủ thể dữ liệu cá nhân;

(3) Về nguồn thu thập dữ liệu cá nhân: Chỉ thu thập những dữ liệu cá nhân cần thiết phục vụ cho hoạt động thông tin tín dụng từ các nguồn phù hợp với quy định của Luật này và các quy định khác của pháp luật có liên quan;

- Chính phủ sẽ quy định chi tiết Điều này.

5. Bảo vệ dữ liệu cá nhân trong kinh doanh dịch vụ quảng cáo

(1) Về nguồn thu thập, sử dụng dữ liệu cá nhân để kinh doanh dịch vụ quảng cáo: Tổ chức, cá nhân kinh doanh dịch vụ quảng cáo chỉ được sử dụng dữ liệu cá nhân từ 02 nguồn, một là từ bên kiểm soát dữ liệu cá nhân, bên kiểm soát và xử lý dữ liệu cá nhân chuyên giao theo thỏa thuận phù hợp quy định pháp luật; hai là thu thập qua hoạt động kinh doanh của chính mình.

(2) Yêu cầu khi xử lý dữ liệu cá nhân của khách hàng để kinh doanh dịch vụ quảng cáo:

+ Phải được sự đồng ý của khách hàng, trên cơ sở khách hàng biết rõ nội dung, phương thức, hình thức, tần suất giới thiệu sản phẩm; cung cấp phương thức cho khách hàng để có thể từ chối nhận các thông tin quảng cáo; cung cấp cơ chế và ngừng quảng cáo theo yêu cầu của chủ thể dữ liệu cá nhân.

+ Phải phù hợp với quy định của pháp luật về phòng, chống tin nhắn rác, thư điện tử rác, cuộc gọi rác và quy định của pháp luật về quảng cáo.

+ Không được thuê lại hoặc thỏa thuận để tổ chức, cá nhân khác thay mặt mình thực hiện toàn bộ dịch vụ quảng cáo có sử dụng dữ liệu cá nhân.

- Trách nhiệm khi sử dụng dữ liệu cá nhân để quảng cáo theo hành vi hoặc có mục tiêu cụ thể hoặc cá nhân hóa quảng cáo:

(1) Chỉ được thu thập dữ liệu cá nhân thông qua việc theo dõi trang thông tin điện tử, công thông tin điện tử, ứng dụng khi có sự đồng ý của chủ thể dữ liệu cá nhân;

(2) Phải thiết lập phương thức cho phép chủ thể dữ liệu cá nhân từ chối chia sẻ dữ liệu; xác định thời gian lưu trữ; xóa, hủy dữ liệu khi không còn cần thiết.

6. Bảo vệ dữ liệu cá nhân đối với các nền tảng mạng xã hội, dịch vụ truyền thông trực tuyến

- Trách nhiệm khi cung cấp dịch vụ mạng xã hội, dịch vụ truyền thông trực tuyến:

(1) Thông báo rõ ràng nội dung dữ liệu cá nhân thu thập khi chủ thể dữ liệu cá nhân cài đặt và sử dụng mạng xã hội, dịch vụ truyền thông trực tuyến; công khai chính sách bảo mật, giải thích rõ cách thức thu thập, sử dụng và chia sẻ dữ liệu cá nhân; không thu thập trái phép dữ liệu cá nhân và ngoài phạm vi theo thỏa thuận với khách hàng;

(2) Không được yêu cầu cung cấp hình ảnh, video chứa nội dung đầy đủ hoặc một phần giấy tờ tùy thân làm yếu tố xác thực tài khoản;

(3) Không nghe lén, nghe trộm hoặc ghi âm cuộc gọi và đọc tin nhắn văn bản khi không có sự đồng ý của chủ thể dữ liệu cá nhân, trừ trường hợp pháp luật có quy định khác;

(4) Bảo vệ dữ liệu cá nhân của công dân Việt Nam khi chuyển dữ liệu xuyên biên giới;

(5) Xây dựng quy trình xử lý vi phạm về bảo vệ dữ liệu cá nhân nhanh chóng và hiệu quả.

- Đối với người dùng, tổ chức, cá nhân cung cấp dịch vụ mạng xã hội, dịch vụ truyền thông trực tuyến phải:

(1) Cung cấp lựa chọn cho phép người dùng từ chối thu thập và chia sẻ tệp dữ liệu (gọi là cookies, với mục đích lưu các hoạt động sử dụng của người dùng trên các trang web từ đó theo dõi hành vi người dùng, cá nhân hóa trải nghiệm, quảng cáo...);

(2) Cung cấp lựa chọn “không theo dõi” hoặc chỉ được theo dõi hoạt động sử dụng mạng xã hội, dịch vụ truyền thông trực tuyến khi có sự đồng ý của người sử dụng;

(3) Cung cấp cho người dùng cơ chế truy cập, chỉnh sửa, xóa dữ liệu và thiết lập quyền riêng tư cho dữ liệu cá nhân, báo cáo các vi phạm về bảo mật và quyền riêng tư.

7. Bảo vệ dữ liệu cá nhân trong xử lý dữ liệu lớn, trí tuệ nhân tạo, chuỗi khối, vũ trụ ảo, điện toán đám mây

- Nguyên tắc xử lý dữ liệu cá nhân trong môi trường dữ liệu lớn, trí tuệ nhân tạo, chuỗi khối, vũ trụ ảo và điện toán đám mây:

+ Xử lý đúng mục đích và giới hạn trong phạm vi cần thiết, bảo đảm quyền, lợi ích hợp pháp của chủ thể dữ liệu cá nhân; phù hợp với chuẩn mực đạo đức, thuần phong mỹ tục của Việt Nam.

+ Không sử dụng, phát triển hệ thống xử lý dữ liệu lớn, trí tuệ nhân tạo, chuỗi khối, vũ trụ ảo, điện toán đám mây có sử dụng dữ liệu cá nhân để gây tổn hại đến quốc phòng, an ninh quốc gia, trật tự, an toàn xã hội hoặc xâm phạm đến tính mạng, sức khỏe, danh dự, nhân phẩm, tài sản của người khác.

- Yêu cầu về biện pháp bảo mật dữ liệu cá nhân: Thực hiện phân loại theo mức độ rủi ro các hệ thống và dịch vụ sử dụng dữ liệu lớn, trí tuệ nhân tạo, chuỗi khối, vũ trụ ảo và điện toán đám mây để tích hợp các biện pháp bảo mật dữ liệu cá nhân phù hợp; phải sử dụng phương thức xác thực, định danh phù hợp và phân quyền truy cập để xử lý dữ liệu cá nhân.

- Chính phủ quy định chi tiết Điều này.

8. Bảo vệ dữ liệu cá nhân đối với dữ liệu vị trí cá nhân, dữ liệu sinh trắc học

- Dữ liệu vị trí cá nhân là dữ liệu được xác định thông qua công nghệ định vị (như GPS, LBS, wifi...) để biết vị trí và giúp xác định con người cụ thể.

- Dữ liệu sinh trắc học là dữ liệu về thuộc tính vật lý, đặc điểm sinh học cá biệt và ổn định của một người để xác định người đó như dấu vân tay, móng mắt, khuôn mặt, giọng nói, mẫu da...

- Yêu cầu bảo vệ dữ liệu vị trí cá nhân:

(1) Không áp dụng việc theo dõi định vị qua thẻ nhận dạng tần số vô tuyến (RFID - là công nghệ cho phép nhận dạng thụ động thông qua việc sử dụng sóng vô tuyến) và các công nghệ khác, trừ trường hợp có sự đồng ý của chủ thể dữ liệu cá nhân hoặc trường hợp có yêu cầu của cơ quan có thẩm quyền theo quy định của pháp luật hoặc trường hợp pháp luật có quy định khác;

(2) Tổ chức, cá nhân cung cấp nền tảng ứng dụng di động phải thông báo cho người sử dụng về việc sử dụng dữ liệu vị trí cá nhân; có biện pháp ngăn chặn việc thu thập dữ liệu vị trí cá nhân của tổ chức, cá nhân không liên quan; cung cấp cho người sử dụng các tùy chọn theo dõi vị trí cá nhân.

- Yêu cầu bảo vệ dữ liệu sinh trắc học:

(1) Phải có biện pháp bảo mật vật lý đối với thiết bị lưu trữ và truyền tải dữ liệu sinh trắc học của mình; hạn chế quyền truy cập vào dữ liệu sinh trắc học; có hệ thống theo dõi để phòng ngừa, phát hiện hành vi xâm phạm dữ liệu sinh trắc học; tuân thủ quy định của pháp luật và tiêu chuẩn quốc tế có liên quan;

(2) Trường hợp xử lý dữ liệu sinh trắc học gây thiệt hại cho chủ thể dữ liệu cá nhân thì tổ chức, cá nhân thu thập và xử lý dữ liệu sinh trắc học phải thông báo cho chủ thể dữ liệu cá nhân đó theo quy định của Chính phủ.

9. Bảo vệ dữ liệu cá nhân thu được từ hoạt động ghi âm, ghi hình tại nơi công cộng, hoạt động công cộng

- Các trường hợp ghi âm, ghi hình và xử lý dữ liệu cá nhân thu được từ hoạt động ghi âm, ghi hình tại nơi công cộng, hoạt động công cộng mà không cần có sự đồng ý của chủ thể dữ liệu cá nhân:

(1) Để thực hiện nhiệm vụ quốc phòng, bảo vệ an ninh quốc gia, bảo đảm trật tự, an toàn xã hội, bảo vệ quyền, lợi ích hợp pháp của cơ quan, tổ chức, cá nhân;

(2) Việc ghi âm, ghi hình từ các hoạt động công cộng bao gồm hội nghị, hội thảo, hoạt động thi đấu thể thao, biểu diễn nghệ thuật và hoạt động công cộng khác mà không làm tổn hại đến danh dự, nhân phẩm, uy tín của chủ thể dữ liệu cá nhân;

(3) Trường hợp khác theo quy định của pháp luật.

Tuy không cần sự đồng ý của chủ thể dữ liệu cá nhân, cơ quan, tổ chức, cá nhân thực hiện ghi âm, ghi hình có trách nhiệm thông báo hoặc bằng hình thức thông tin khác để chủ thể dữ liệu cá nhân biết được mình đang bị ghi âm, ghi hình, trừ trường hợp pháp luật có quy định khác.

- Dữ liệu cá nhân thu được chỉ được:

+ Xử lý, sử dụng phù hợp với mục đích xử lý, không được sử dụng vào các mục đích trái pháp luật hoặc xâm phạm đến quyền, lợi ích hợp pháp của chủ thể dữ liệu cá nhân;

+ Lưu trữ trong khoảng thời gian cần thiết để phục vụ mục đích thu thập, trừ trường hợp pháp luật có quy định khác. Khi hết thời hạn lưu trữ, dữ liệu cá nhân phải được xóa, hủy theo quy định của Luật này.

Chương III

LỰC LƯỢNG, ĐIỀU KIỆN BẢO ĐẢM BẢO VỆ DỮ LIỆU CÁ NHÂN

1. Lực lượng bảo vệ dữ liệu cá nhân

- Lực lượng bảo vệ dữ liệu cá nhân bao gồm:

(1) Cơ quan chuyên trách bảo vệ dữ liệu cá nhân thuộc Bộ Công an;

(2) Bộ phận, nhân sự bảo vệ dữ liệu cá nhân trong cơ quan, tổ chức;

(3) Tổ chức, cá nhân cung cấp dịch vụ bảo vệ dữ liệu cá nhân;

(4) Tổ chức, cá nhân được huy động tham gia bảo vệ dữ liệu cá nhân.

- Cơ quan, tổ chức có trách nhiệm chỉ định bộ phận, nhân sự đủ điều kiện năng lực bảo vệ dữ liệu cá nhân hoặc thuê tổ chức, cá nhân cung cấp dịch vụ bảo vệ dữ liệu cá nhân.

- Chính phủ quy định về điều kiện, nhiệm vụ của bộ phận, nhân sự bảo vệ dữ liệu cá nhân trong cơ quan, tổ chức; tổ chức, cá nhân cung cấp dịch vụ bảo vệ dữ liệu cá nhân; dịch vụ xử lý dữ liệu cá nhân.

2. Tiêu chuẩn, quy chuẩn kỹ thuật về bảo vệ dữ liệu cá nhân

- Tiêu chuẩn về bảo vệ dữ liệu cá nhân gồm tiêu chuẩn đối với hệ thống thông tin, phần cứng, phần mềm, quản lý, vận hành, xử lý, bảo vệ dữ liệu cá nhân được công bố, thừa nhận áp dụng tại Việt Nam.

- Quy chuẩn kỹ thuật về bảo vệ dữ liệu cá nhân gồm quy chuẩn kỹ thuật đối với hệ thống thông tin, phần cứng, phần mềm, quản lý, vận hành, xử lý, bảo vệ dữ liệu cá nhân được xây dựng, ban hành và áp dụng tại Việt Nam.

3. Kiểm tra hoạt động bảo vệ dữ liệu cá nhân

Chính phủ sẽ quy định chi tiết việc kiểm tra hoạt động bảo vệ dữ liệu cá nhân, trong đó việc kiểm tra được thực hiện khi có hành vi vi phạm pháp luật về bảo vệ dữ liệu cá nhân và để thực hiện công tác quản lý nhà nước theo quy định của pháp luật.

Chương IV

TRÁCH NHIỆM CỦA CƠ QUAN, TỔ CHỨC, CÁ NHÂN VỀ BẢO VỆ DỮ LIỆU CÁ NHÂN

1. Trách nhiệm quản lý nhà nước về bảo vệ dữ liệu cá nhân

- Chính phủ thống nhất thực hiện quản lý nhà nước về bảo vệ dữ liệu cá nhân.
- Bộ Công an là cơ quan đầu mối chịu trách nhiệm trước Chính phủ thực hiện quản lý nhà nước về bảo vệ dữ liệu cá nhân, trừ nội dung thuộc phạm vi quản lý của Bộ Quốc phòng.
- Bộ Quốc phòng chịu trách nhiệm trước Chính phủ thực hiện quản lý nhà nước về bảo vệ dữ liệu cá nhân thuộc phạm vi quản lý.
- Bộ, cơ quan ngang Bộ, cơ quan thuộc Chính phủ thực hiện quản lý nhà nước về bảo vệ dữ liệu cá nhân đối với các ngành, lĩnh vực thuộc phạm vi quản lý theo quy định của pháp luật và chức năng, nhiệm vụ được giao.
- Ủy ban nhân dân cấp tỉnh thực hiện quản lý nhà nước về bảo vệ dữ liệu cá nhân theo quy định của pháp luật và chức năng, nhiệm vụ được giao.

2. Trách nhiệm của bên kiểm soát dữ liệu cá nhân, bên xử lý dữ liệu cá nhân, bên kiểm soát và xử lý dữ liệu cá nhân

- Trách nhiệm của bên kiểm soát dữ liệu cá nhân như sau:
 - (1) Nêu rõ trách nhiệm, quyền và nghĩa vụ phải tuân thủ của các bên trong thỏa thuận, hợp đồng có liên quan đến xử lý dữ liệu cá nhân theo quy định của Luật này và quy định khác của pháp luật có liên quan;
 - (2) Quyết định mục đích và phương tiện xử lý dữ liệu cá nhân tại các văn bản, thỏa thuận với chủ thể dữ liệu cá nhân, bảo đảm đúng nguyên tắc và nội dung theo quy định của Luật này;
 - (3) Thực hiện biện pháp quản lý, kỹ thuật phù hợp để bảo vệ dữ liệu cá nhân theo quy định của pháp luật, rà soát và cập nhật các biện pháp này khi cần thiết;
 - (4) Thông báo hành vi vi phạm quy định về bảo vệ dữ liệu cá nhân;
 - (5) Lựa chọn bên xử lý dữ liệu cá nhân phù hợp để xử lý dữ liệu cá nhân;

(6) Bảo đảm các quyền của chủ thể dữ liệu cá nhân;

(7) Chịu trách nhiệm trước chủ thể dữ liệu cá nhân về các thiệt hại do quá trình xử lý dữ liệu cá nhân gây ra;

(8) Ngăn chặn hoạt động thu thập dữ liệu cá nhân trái phép từ hệ thống, trang thiết bị, dịch vụ của mình;

(9) Phối hợp với Bộ Công an, cơ quan nhà nước có thẩm quyền trong bảo vệ dữ liệu cá nhân, cung cấp thông tin phục vụ điều tra, xử lý hành vi vi phạm pháp luật về bảo vệ dữ liệu cá nhân;

- Trách nhiệm của bên xử lý dữ liệu cá nhân như sau:

(1) Chỉ được tiếp nhận dữ liệu cá nhân sau khi có thỏa thuận, hợp đồng về xử lý dữ liệu cá nhân với bên kiểm soát dữ liệu cá nhân, bên kiểm soát và xử lý dữ liệu cá nhân;

(2) Xử lý dữ liệu cá nhân theo đúng thỏa thuận, hợp đồng ký kết với bên kiểm soát dữ liệu cá nhân, bên kiểm soát và xử lý dữ liệu cá nhân;

(3) Thực hiện đầy đủ các biện pháp bảo vệ dữ liệu cá nhân theo quy định của Luật này và các quy định khác của pháp luật có liên quan;

(4) Chịu trách nhiệm trước bên kiểm soát dữ liệu cá nhân, bên kiểm soát và xử lý dữ liệu cá nhân về thiệt hại do quá trình xử lý dữ liệu cá nhân gây ra;

(5) Ngăn chặn hoạt động thu thập dữ liệu cá nhân trái phép từ hệ thống, trang thiết bị, dịch vụ của mình;

(6) Phối hợp với Bộ Công an, cơ quan nhà nước có thẩm quyền trong bảo vệ dữ liệu cá nhân, cung cấp thông tin phục vụ điều tra, xử lý hành vi vi phạm pháp luật về bảo vệ dữ liệu cá nhân;

(7) Thực hiện các trách nhiệm khác theo quy định của Luật này và quy định khác của pháp luật có liên quan.

- Bên kiểm soát và xử lý dữ liệu cá nhân có trách nhiệm thực hiện đầy đủ các nghĩa vụ của bên kiểm soát và bên xử lý.

Chương V

ĐIỀU KHOẢN THI HÀNH

1. Hiệu lực thi hành

- Luật này có hiệu lực thi hành từ ngày 01 tháng 01 năm 2026.

- Doanh nghiệp nhỏ, doanh nghiệp khởi nghiệp được quyền lựa chọn thực hiện hoặc không thực hiện quy định về đánh giá tác động xử lý dữ liệu cá nhân và chỉ định bộ phận, nhân sự đủ điều kiện năng lực bảo vệ dữ liệu cá nhân hoặc thuê tổ chức, cá nhân cung cấp dịch vụ bảo vệ dữ liệu cá nhân trong thời gian 05 năm kể từ ngày Luật này có hiệu lực thi hành,

Đối tượng loại trừ: doanh nghiệp nhỏ, doanh nghiệp khởi nghiệp kinh doanh dịch vụ xử lý dữ liệu cá nhân, trực tiếp xử lý dữ liệu cá nhân nhạy cảm hoặc xử lý dữ liệu cá nhân của số lượng lớn chủ thể dữ liệu cá nhân.

- Hộ kinh doanh, doanh nghiệp siêu nhỏ không phải thực hiện quy định quy định về đánh giá tác động xử lý dữ liệu cá nhân và chỉ định bộ phận, nhân sự đủ điều kiện năng lực bảo vệ dữ liệu cá nhân hoặc thuê tổ chức, cá nhân cung cấp dịch vụ bảo vệ dữ liệu cá nhân

Đối tượng loại trừ: hộ kinh doanh, doanh nghiệp siêu nhỏ kinh doanh dịch vụ xử lý dữ liệu cá nhân, trực tiếp xử lý dữ liệu cá nhân nhạy cảm hoặc xử lý dữ liệu cá nhân của số lượng lớn chủ thể dữ liệu cá nhân.

- Chính phủ quy định chi tiết các nội dung này.

2. Quy định chuyển tiếp

- Hoạt động xử lý dữ liệu cá nhân đang thực hiện mà đã được chủ thể dữ liệu cá nhân đồng ý hoặc theo thỏa thuận theo quy định của Nghị định số 13/2023/NĐ-CP ngày 17 tháng 4 năm 2023 của Chính phủ trước ngày Luật này có hiệu lực thi hành thì tiếp tục thực hiện, không phải xin đồng ý lại hoặc thỏa thuận lại.

- Hồ sơ đánh giá tác động xử lý dữ liệu cá nhân, hồ sơ đánh giá tác động chuyển dữ liệu cá nhân ra nước ngoài theo quy định của Nghị định số 13/2023/NĐ-CP ngày 17 tháng 4 năm 2023 của Chính phủ đã được cơ quan chuyên trách bảo vệ dữ liệu cá nhân tiếp nhận trước ngày Luật này có hiệu lực thi hành thì tiếp tục được sử dụng và không phải lập 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 theo quy định của Luật này; việc cập nhật các hồ sơ đã lập nêu trên sau ngày Luật này có hiệu lực thi hành thì thực hiện theo quy định của Luật này.

III. Các điều kiện đảm bảo thực hiện

Quy định của Luật không làm tăng tổ chức bộ máy và biên chế hưởng lương từ ngân sách nhà nước nên sau khi dự án Luật được thông qua, nguồn nhân lực bảo đảm thi hành là đội ngũ nhân lực đang thực hiện nhiệm vụ triển khai thi hành Luật hiện nay của các cơ quan, đơn vị.

Để triển khai thi hành Luật, Nhà nước cần đầu tư một khoản kinh phí cho việc tổ chức thực hiện; cụ thể là:

- Tuyên truyền, phổ biến nội dung của Luật, tổ chức các đợt tập huấn, tập huấn chuyên sâu cho những người làm công tác bảo vệ dữ liệu cá nhân.

- Chi phí đầu tư mua sắm trang thiết bị, phương tiện bảo vệ dữ liệu cá nhân; kiện toàn, củng cố, xây dựng lực lượng bảo vệ dữ liệu cá nhân.

- Ban hành, in ấn, cấp phát sổ sách, biểu mẫu, giấy tờ và các tài liệu phục vụ công tác bảo vệ dữ liệu cá nhân.

- Chi phí phục vụ việc theo dõi, tổng kết, đánh giá tình hình thực thi luật hàng năm.

IV. Triển khai thi hành

Để tổ chức thi hành Luật hiệu quả, theo sự phân công của Chính phủ, Bộ Công an sẽ chủ trì, phối hợp với các bộ, ngành, địa phương xây dựng văn bản hướng dẫn thi hành; đồng thời, trong thời gian tới, trên cơ sở Kế hoạch triển khai thi hành Luật của Thủ tướng Chính phủ, Bộ Công an sẽ tổ chức phổ biến, hướng dẫn cho các bộ, ngành, địa phương, tổ chức, cá nhân về Luật Bảo vệ dữ liệu cá nhân. Từ đó, nhận thức xã hội về bảo vệ dữ liệu cá nhân, các quyền và nghĩa vụ của chủ thể dữ liệu, trách nhiệm của các bên liên quan trong hoạt động xử lý được nâng cao; góp phần bảo vệ quyền riêng tư, quyền con người, đấu tranh phòng, chống các hành vi vi phạm pháp luật về bảo vệ dữ liệu cá nhân./.