

NGHỊ ĐỊNH

Quy định chi tiết một số điều và biện pháp thi hành Luật Dữ liệu

Căn cứ Luật Tổ chức Chính phủ ngày 18 tháng 02 năm 2025;

Căn cứ Luật Dữ liệu ngày 30 tháng 11 năm 2024;

Theo đề nghị của Bộ trưởng Bộ Công an;

Chính phủ ban hành Nghị định quy định chi tiết và biện pháp thi hành Luật Dữ liệu.

Chương I
QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh

Nghị định này quy định chi tiết khoản 3 Điều 13, khoản 5 Điều 14, khoản 5 Điều 15, khoản 3 Điều 16, khoản 4 Điều 17, khoản 4 Điều 18, khoản 3 Điều 20, khoản 5 Điều 21, khoản 5 Điều 22, khoản 4 Điều 23, khoản 5 Điều 25, khoản 4 Điều 26, khoản 4 Điều 27, khoản 3 Điều 30, khoản 8 Điều 31, khoản 5 Điều 35, khoản 4 Điều 36, khoản 3 Điều 37 của Luật Dữ liệu và việc xây dựng, phát triển, bảo vệ, quản trị, xử lý, sử dụng dữ liệu; việc bảo đảm nguồn lực cho hoạt động của Trung tâm dữ liệu quốc gia; trách nhiệm của cơ quan, tổ chức, cá nhân có liên quan đến hoạt động về dữ liệu.

Điều 2. Đối tượng áp dụng

- Cơ quan, tổ chức, cá nhân Việt Nam.
- Cơ quan, tổ chức, cá nhân nước ngoài tại Việt Nam.
- Cơ quan, tổ chức, cá nhân nước ngoài trực tiếp tham gia hoặc có liên quan đến hoạt động dữ liệu số tại Việt Nam.

Chương II
CÁC HOẠT ĐỘNG XỬ LÝ DỮ LIỆU

Điều 3. Tiêu chí xác định dữ liệu quan trọng

Việc xác định dữ liệu quan trọng căn cứ theo mức độ có thể tác động của dữ liệu đến quốc phòng, an ninh, cơ yếu, đối ngoại, kinh tế vĩ mô, ổn định xã hội, sức khỏe và an toàn cộng đồng khi bị thu thập, sử dụng trái phép (không bao gồm bí mật nhà nước), bao gồm:

1. Dữ liệu có thể gây tác động nguy hiểm đến an ninh quốc gia, độc lập, chủ quyền, thống nhất và toàn vẹn lãnh thổ của Tổ quốc, bảo vệ Đảng, Nhà nước, khối đại đoàn kết toàn dân tộc; bảo vệ an ninh chính trị, an ninh trong các lĩnh vực tư tưởng - văn hóa, kinh tế, quốc phòng, đối ngoại, thông tin, xã hội, tài nguyên, môi trường, nông nghiệp, sinh học, y tế, lao động, xây dựng, giáo dục, đào tạo, khoa học và công nghệ.

2. Dữ liệu có thể gây tác động nguy hiểm đến kế hoạch phát triển quan hệ đối ngoại, ảnh hưởng lợi ích quốc gia và an ninh hợp tác quốc tế, dự án đầu tư của Việt Nam ở nước ngoài, an ninh năng lượng, hàng hải.

3. Dữ liệu có thể gây tác động nguy hiểm đến phát triển, vận hành kinh tế vĩ mô, ngành kinh tế quan trọng của quốc gia, tổng cung, tổng cầu của xã hội, tổng giá trị kinh tế quốc gia, tỷ lệ thất nghiệp, lĩnh vực tiền tệ, thương mại, xuất, nhập khẩu, cung ứng hàng hóa, sản phẩm, dịch vụ thiết yếu.

4. Dữ liệu có thể gây tác động nguy hiểm đến tính mạng, sức khỏe, danh dự, nhân phẩm, tài sản, quyền, lợi ích hợp pháp của cơ quan, tổ chức, cá nhân; công tác phòng chống dịch bệnh, phòng ngừa, theo dõi và điều trị các bệnh truyền nhiễm, bệnh nghề nghiệp, an toàn vệ sinh thực phẩm; cung ứng lao động, cung cấp các dịch vụ công.

Điều 4. Tiêu chí xác định dữ liệu cốt lõi

Việc xác định dữ liệu cốt lõi căn cứ vào tác động trực tiếp của dữ liệu gây nguy hiểm đến quốc phòng, an ninh, cơ yếu, đối ngoại, kinh tế vĩ mô, ổn định xã hội, sức khỏe và an toàn cộng đồng khi bị thu thập, sử dụng trái phép (không bao gồm bí mật nhà nước), bao gồm:

1. Dữ liệu trực tiếp gây tác động nguy hiểm đến an ninh quốc gia, độc lập, chủ quyền, thống nhất và toàn vẹn lãnh thổ của Tổ quốc, bảo vệ Đảng, Nhà nước, khối đại đoàn kết toàn dân tộc; bảo vệ an ninh chính trị, an ninh trong các lĩnh vực tư tưởng - văn hóa, kinh tế, quốc phòng, đối ngoại, thông tin, xã hội, tài nguyên, môi trường, nông nghiệp, sinh học, y tế, lao động, xây dựng, giáo dục, đào tạo, khoa học và công nghệ.

2. Dữ liệu trực tiếp gây tác động nguy hiểm đến kế hoạch phát triển quan hệ đối ngoại, ảnh hưởng lợi ích quốc gia và an ninh hợp tác quốc tế, dự án đầu tư của Việt Nam ở nước ngoài, an ninh năng lượng, hàng hải.

3. Dữ liệu trực tiếp gây tác động nguy hiểm đến phát triển, vận hành kinh tế vĩ mô, ngành kinh tế quan trọng của quốc gia, tổng cung, tổng cầu của xã hội, tổng giá trị kinh tế quốc gia, tỷ lệ thất nghiệp, lĩnh vực tiền tệ, thương mại, xuất, nhập khẩu, cung ứng hàng hóa, sản phẩm, dịch vụ thiết yếu.

4. Dữ liệu trực tiếp gây tác động nguy hiểm đến tính mạng, sức khỏe, danh dự, nhân phẩm, tài sản, quyền, lợi ích hợp pháp của cơ quan, tổ chức, cá nhân;

công tác phòng chống dịch bệnh, phòng ngừa, theo dõi và điều trị các bệnh truyền nhiễm, bệnh nghề nghiệp, an toàn vệ sinh thực phẩm; cung ứng lao động, cung cấp các dịch vụ công.

Điều 5. Hoạt động lưu trữ dữ liệu

1. Chủ sở hữu dữ liệu quy định thời hạn lưu trữ cụ thể đối với dữ liệu do mình thu thập, tạo lập.

2. Cơ quan nhà nước phải ban hành quy trình kỹ thuật về lưu trữ dữ liệu do mình quản lý, bảo đảm lưu trữ dữ liệu an toàn.

3. Trung tâm dữ liệu quốc gia thiết lập các dịch vụ lưu trữ dữ liệu phục vụ nhu cầu của chủ sở hữu dữ liệu, chủ quản dữ liệu. Chủ sở hữu dữ liệu, chủ quản dữ liệu phối hợp với Trung tâm dữ liệu quốc gia xây dựng kế hoạch, lộ trình thực hiện theo dịch vụ lưu trữ dữ liệu cụ thể.

Điều 6. Truy cập, truy xuất dữ liệu

1. Truy cập dữ liệu là hoạt động tiếp cận, tác động tới dữ liệu theo đúng quyền được giao, bao gồm truy cập đọc, truy cập ghi, truy cập sửa, truy cập xóa, truy cập thực thi và các loại truy cập khác do chủ sở hữu dữ liệu, chủ quản dữ liệu quy định.

2. Truy xuất dữ liệu là hoạt động truy cập và trích xuất dữ liệu, bao gồm truy xuất thủ công, truy xuất tự động, truy xuất theo thời gian thực và các loại truy xuất khác do chủ sở hữu dữ liệu, chủ quản dữ liệu quy định.

3. Nguyên tắc thực hiện truy cập, truy xuất dữ liệu:

- a) Bảo đảm hợp pháp, tuân thủ quy trình truy cập, truy xuất dữ liệu;
- b) Chỉ truy cập, truy xuất dữ liệu trong phạm vi quyền được giao và cần thiết cho mục đích được xác định.

4. Cơ quan nhà nước phải ban hành quy trình kỹ thuật về truy cập, truy xuất dữ liệu đối với dữ liệu thuộc phạm vi quản lý, gồm các nội dung chính sau:

- a) Quản lý thông tin đăng ký sử dụng;
- b) Quản lý phân quyền truy cập, truy xuất dữ liệu;
- c) Quản lý lịch sử truy cập, truy xuất dữ liệu;
- d) Quản lý công cụ truy cập, truy xuất dữ liệu.

Điều 7. Hỗ trợ chủ sở hữu dữ liệu thực hiện kết nối, chia sẻ dữ liệu cho cơ quan nhà nước

Cơ quan nhà nước thực hiện các biện pháp hỗ trợ chủ sở hữu dữ liệu kết nối, chia sẻ dữ liệu cho cơ quan nhà nước gồm:

- 1. Xây dựng hệ thống thông tin bảo đảm việc kết nối, chia sẻ dữ liệu; bảo

vệ, sử dụng dữ liệu đã được chủ sở hữu dữ liệu chia sẻ theo đúng mục đích đã được xác định.

2. Xây dựng các quy trình, ứng dụng, phần mềm để chủ sở hữu dữ liệu thực hiện các quyền của mình đối với dữ liệu đã cung cấp cho cơ quan nhà nước theo quy định của pháp luật.

3. Bộ trưởng, Thủ trưởng cơ quan ngang bộ, cơ quan thuộc Chính phủ, Chủ tịch Ủy ban nhân dân các tỉnh, thành phố trực thuộc trung ương quyết định việc hỗ trợ cho chủ sở hữu dữ liệu, bao gồm:

a) Hỗ trợ đường truyền kết nối; hỗ trợ các công cụ để bảo đảm đáp ứng tiêu chuẩn kỹ thuật kết nối, chia sẻ; hỗ trợ hạ tầng, an ninh an toàn bảo mật;

b) Hỗ trợ kinh phí bảo đảm kết nối, chia sẻ; hỗ trợ bù đắp chi phí tạo lập, thu thập dữ liệu theo định mức của cơ quan nhà nước;

c) Hỗ trợ nhân lực thực hiện kết nối, chia sẻ dữ liệu; hỗ trợ đào tạo, tập huấn nguồn nhân lực phục vụ kết nối, chia sẻ dữ liệu;

d) Các hình thức hỗ trợ khác.

Điều 8. Cung cấp dữ liệu cho cơ quan nhà nước

1. Khuyến khích cá nhân, tổ chức chia sẻ, cung cấp dữ liệu của mình cho cơ quan nhà nước cho các mục tiêu vì lợi ích chung như chăm sóc sức khỏe, biến đổi khí hậu, cải thiện giao thông, tạo điều kiện cho việc tổng hợp và phổ biến số liệu thống kê chính thức, cải thiện việc cung cấp dịch vụ công, hoạch định chính sách công hoặc mục đích nghiên cứu khoa học.

Tổ chức, cá nhân chia sẻ, cung cấp dữ liệu một cách tự nguyện trên cơ sở có sự đồng ý của chủ thể dữ liệu để xử lý dữ liệu cá nhân liên quan đến họ hoặc sự cho phép của chủ sở hữu dữ liệu để cho phép sử dụng dữ liệu phi cá nhân của họ.

2. Cơ quan nhà nước yêu cầu tổ chức, cá nhân cung cấp dữ liệu theo quy định tại khoản 2 Điều 18 Luật Dữ liệu như sau:

a) Có văn bản yêu cầu hoặc hình thức khác bảo đảm có xác nhận về việc yêu cầu cung cấp dữ liệu trong đó chỉ rõ loại dữ liệu, mức độ chi tiết, khối lượng dữ liệu, tần suất truy cập dữ liệu, phương thức cung cấp dữ liệu, cơ sở pháp lý, căn cứ, lý do của yêu cầu, mục đích sử dụng dữ liệu, thời hạn sử dụng và thời hạn cần cung cấp dữ liệu, các hoạt động xử lý dữ liệu dự kiến sẽ thực hiện;

b) Thông báo cho tổ chức, cá nhân được yêu cầu cung cấp dữ liệu về các chế tài sẽ được áp dụng trong trường hợp không thực hiện yêu cầu.

3. Bàn giao, tiếp nhận dữ liệu được yêu cầu

a) Việc bàn giao, tiếp nhận dữ liệu được thực hiện theo đúng đối tượng,

thời gian, loại dữ liệu, mức độ chi tiết, khối lượng dữ liệu, tần suất truy cập dữ liệu, phương thức cung cấp dữ liệu được yêu cầu cung cấp;

b) Thành phần tham gia bàn giao, tiếp nhận dữ liệu gồm có Chủ sở hữu dữ liệu, người đại diện hợp pháp hoặc người đang quản lý, sử dụng hợp pháp dữ liệu; cá nhân, đại diện tổ chức được giao quản lý, sử dụng dữ liệu;

c) Việc bàn giao, tiếp nhận dữ liệu phải được lập thành biên bản;

d) Bên yêu cầu cung cấp dữ liệu có quyền yêu cầu bên cung cấp dữ liệu bổ sung dữ liệu trong trường hợp dữ liệu bàn giao không đúng với phạm vi dữ liệu được yêu cầu cung cấp.

4. Hủy bỏ yêu cầu cung cấp dữ liệu

a) Yêu cầu cung cấp dữ liệu bị hủy bỏ trong các trường hợp yêu cầu cung cấp dữ liệu trái với quy định của Luật Dữ liệu và các luật khác có liên quan; yêu cầu cung cấp dữ liệu chưa được thực hiện nhưng điều kiện cung cấp dữ liệu quy định tại khoản 1 Điều 18 Luật Dữ liệu không còn; yêu cầu cung cấp dữ liệu chưa được thực hiện nhưng vì lý do khách quan mà dữ liệu không còn tồn tại;

b) Việc hủy bỏ yêu cầu cung cấp dữ liệu phải được thể hiện bằng văn bản.

5. Yêu cầu sửa đổi, rút lại yêu cầu cung cấp dữ liệu

a) Trước thời hạn chỉ định cần cung cấp dữ liệu, chủ sở hữu dữ liệu, người đại diện hợp pháp hoặc người đang quản lý, sử dụng hợp pháp dữ liệu có thể yêu cầu cơ quan có thẩm quyền sửa đổi, rút lại yêu cầu cung cấp dữ liệu;

b) Chủ sở hữu dữ liệu, chủ quản dữ liệu có thể yêu cầu sửa đổi, rút lại yêu cầu cung cấp dữ liệu trong các trường hợp yêu cầu cung cấp dữ liệu trái với quy định của Luật Dữ liệu và các luật khác có liên quan; phạm vi dữ liệu quản lý của chủ sở hữu dữ liệu, chủ quản dữ liệu không nằm trong yêu cầu cung cấp dữ liệu; vì lý do khách quan mà dữ liệu không còn tồn tại.

6. Thẩm quyền yêu cầu cung cấp dữ liệu

Bộ trưởng, Thủ trưởng cơ quan ngang bộ, Chủ tịch Ủy ban nhân dân tỉnh, thành phố trực thuộc trung ương, Giám đốc Trung tâm dữ liệu quốc gia, Giám đốc Công an tỉnh, thành phố trực thuộc trung ương có thẩm quyền yêu cầu cung cấp dữ liệu trong phạm vi nhiệm vụ, quyền hạn của mình.

Điều 9. Xác nhận, xác thực dữ liệu

1. Xác nhận dữ liệu được thực hiện như sau:

a) Dữ liệu được thu thập, cập nhật vào cơ sở dữ liệu quốc gia, cơ sở dữ liệu chuyên ngành; cơ sở dữ liệu khác được xác nhận bởi chủ sở hữu dữ liệu, chủ quản dữ liệu;

b) Việc xác nhận dữ liệu giữa các cơ quan nhà nước, tổ chức chính trị - xã hội thực hiện thông qua quy chế phối hợp và phương thức kết nối, chia sẻ, cung cấp dữ liệu;

c) Ngoài trường hợp quy định tại điểm a và điểm b khoản này, việc xác nhận dữ liệu được thực hiện theo thỏa thuận giữa người dùng dữ liệu với chủ quản dữ liệu, chủ sở hữu dữ liệu hoặc tổ chức khác theo quy định của pháp luật;

d) Chủ sở hữu dữ liệu, chủ quản dữ liệu chịu trách nhiệm về chất lượng dữ liệu, mức độ tin cậy, hợp pháp của dữ liệu do mình cung cấp, xác nhận; xây dựng quy trình, hình thức và tổ chức hoạt động xác nhận dữ liệu.

2. Chủ sở hữu dữ liệu, chủ quản dữ liệu có trách nhiệm tự xây dựng quy trình, hình thức và tổ chức hoạt động xác thực dữ liệu trong phạm vi mình sở hữu, quản lý.

3. Phạm vi và thời gian của việc xác thực dữ liệu do chủ sở hữu dữ liệu quyết định.

4. Việc xác nhận, xác thực dữ liệu thực hiện theo quy định của pháp luật về xác thực điện tử và quy định của pháp luật có liên quan.

Điều 10. Công khai dữ liệu

1. Việc công khai dữ liệu mở được thực hiện ngay sau khi dữ liệu được phân loại là dữ liệu mở. Chủ sở hữu dữ liệu, chủ quản dữ liệu thực hiện công khai dữ liệu mở dưới hình thức:

a) Cổng dữ liệu quốc gia;

b) Các cổng dữ liệu mở, cổng thông tin điện tử của bộ, ngành, địa phương và các hệ thống, nền tảng khác;

c) Các hệ thống trung gian phục vụ kết nối, chia sẻ dữ liệu hoặc các hình thức khác theo quy định của pháp luật.

2. Cơ quan nhà nước có trách nhiệm công bố danh mục dữ liệu mở và tổ chức công khai dữ liệu mở do mình quản lý và gửi Bộ Công an tổng hợp, đăng tải trên Cổng dữ liệu quốc gia.

3. Dữ liệu của cơ quan nhà nước không thuộc diện bị cấm công khai do liên quan đến an ninh quốc gia, quyền riêng tư, bí mật thương mại hoặc các lý do khác theo quy định của pháp luật phải được công khai như dữ liệu mở.

4. Cơ quan nhà nước xây dựng, triển khai quyết định công bố dữ liệu mở, trong đó xác định danh mục dữ liệu mở công bố, cơ chế thu thập, phân tích thông tin phản hồi của cá nhân, tổ chức về việc sử dụng dữ liệu mở; đánh giá chất lượng, tính khả dụng, việc tuân thủ các quy định pháp luật liên quan đến dữ liệu mở.

Điều 11. Mã hóa, giải mã dữ liệu

1. Cơ quan, tổ chức, cá nhân được sử dụng một hoặc nhiều giải pháp mã hóa và quy trình mã hóa, giải mã phù hợp với hoạt động quản trị, quản lý dữ liệu của mình gồm:

- a) Giải pháp mã hóa dữ liệu khi truyền tải dữ liệu;
- b) Giải pháp mã hóa dữ liệu khi lưu trữ dữ liệu;
- c) Giải pháp mã hóa dữ liệu trên thiết bị số;
- d) Giải pháp bảo mật phần cứng nhằm phòng chống truy cập trái phép và bảo đảm rằng các thao tác mã hóa/giải mã chỉ được thực hiện trong môi trường an toàn;
- đ) Quy trình giải mã yêu cầu xác thực danh người thực hiện giải mã dữ liệu, xác định và cấp quyền truy cập dữ liệu đã được mã hóa;
- e) Giải pháp ghi lại các hoạt động mã hóa và giải mã nhằm bảo đảm tính hợp pháp, minh bạch, công bằng và phục vụ tra cứu;
- g) Các giải pháp, quy trình khác theo quy định của pháp luật.

2. Bộ trưởng Bộ Công an quyết định hoặc phân cấp việc quyết định áp dụng các biện pháp để giải mã dữ liệu đối với các trường hợp quy định tại khoản 4 Điều 22 Luật Dữ liệu mà không cần chủ sở hữu dữ liệu, chủ quản dữ liệu đồng ý, trừ trường hợp thuộc lĩnh vực quân sự, quốc phòng.

3. Bộ trưởng Bộ Quốc phòng quyết định hoặc phân cấp việc quyết định áp dụng các biện pháp để giải mã dữ liệu liên quan tới quân sự, quốc phòng đối với các trường hợp quy định tại khoản 4 Điều 22 Luật Dữ liệu mà không cần chủ sở hữu dữ liệu, chủ quản dữ liệu đồng ý.

Điều 12. Chuyển, xử lý dữ liệu xuyên biên giới

1. Chủ sở hữu dữ liệu, chủ quản dữ liệu khi cần chuyển, xử lý dữ liệu cốt lõi, dữ liệu quan trọng xuyên biên giới thì thực hiện đánh giá tác động theo quy định khoản 2 Điều này.

Đánh giá tác động chuyển dữ liệu cốt lõi, quan trọng ra nước ngoài, cho tổ chức, cá nhân nước ngoài được thực hiện 01 lần cho suốt thời gian hoạt động của tổ chức, doanh nghiệp và được cập nhật, bổ sung theo quy định tại khoản 8 Điều này.

2. Bên chuyển dữ liệu phải đánh giá tác động với các vấn đề sau:

- a) Tính hợp pháp, sự cần thiết, phạm vi, phương thức truyền dữ liệu và cách xử lý dữ liệu của bên nhận dữ liệu;
- b) Những rủi ro mà việc chuyển dữ liệu có thể gây ra cho quốc phòng, an ninh, hoạt động kinh tế, đối ngoại, ổn định xã hội, lợi ích công cộng hoặc quyền

và lợi ích hợp pháp của cá nhân hoặc tổ chức; rủi ro dữ liệu sẽ bị giả mạo, phá hủy, rò rỉ, mất hoặc sử dụng bất hợp pháp;

c) Trách nhiệm và nghĩa vụ, các biện pháp quản lý, kỹ thuật của bên nhận dữ liệu;

d) Các vấn đề khác có liên quan.

3. Văn bản giao kết giữa bên chuyển dữ liệu và bên nhận dữ liệu, phải xác định rõ:

a) Mục đích, phương pháp và phạm vi xuất dữ liệu, mục đích và phương pháp xử lý dữ liệu của bên nhận dữ liệu;

b) Địa điểm và thời gian lưu trữ dữ liệu, các biện pháp xử lý dữ liệu sau khi hết thời hạn lưu trữ, hoàn thành mục tiêu đã thỏa thuận;

c) Yêu cầu ràng buộc đối với bên nhận dữ liệu về việc cung cấp dữ liệu đã được chuyển giao cho bên thứ ba;

d) Các biện pháp bảo vệ dữ liệu mà bên nhận dữ liệu sẽ sử dụng;

đ) Biện pháp khắc phục hậu quả, bồi thường thiệt hại, trách nhiệm xử lý vi phạm hợp đồng, biện pháp giải quyết tranh chấp đối với hành vi phạm nghĩa vụ bảo vệ dữ liệu;

e) Trách nhiệm của các bên trong việc xử lý dữ liệu.

4. Hồ sơ đánh giá tác động chuyển, xử lý dữ liệu xuyên biên giới gồm Báo cáo đánh giá tác động chuyển, xử lý dữ liệu xuyên biên giới (theo Mẫu số 02 ban hành kèm theo Nghị định này) và các văn bản khác có liên quan.

5. Trường hợp dữ liệu chuyển, xử lý ở nước ngoài là dữ liệu cốt lõi:

a) Bên chuyển dữ liệu gửi hồ sơ đánh giá tác động chuyển, xử lý dữ liệu xuyên biên giới đến Bộ Công an, trường hợp thuộc lĩnh vực quân sự, quốc phòng, cơ yếu thì gửi hồ sơ về Bộ Quốc phòng;

b) Đơn vị chịu trách nhiệm thuộc Bộ Quốc phòng, Bộ Công an nhận hồ sơ kiểm tra tính đầy đủ, hợp lệ của hồ sơ. Trường hợp hồ sơ chưa đầy đủ thì yêu cầu bên chuyển dữ liệu bổ sung, hoàn thiện hồ sơ;

c) Đơn vị chịu trách nhiệm thuộc Bộ Quốc phòng, Bộ Công an hoàn thành việc đánh giá hồ sơ đánh giá tác động chuyển, xử lý dữ liệu ra nước ngoài trong thời hạn 10 ngày kể từ ngày nhận được hồ sơ đầy đủ, hợp lệ; trường hợp hồ sơ phức tạp, cần xác minh, kiểm tra thì không quá 15 ngày;

d) Bên chuyển dữ liệu phải được thông báo bằng văn bản về kết quả đánh giá. Sau khi nhận được kết quả đánh giá đạt, chủ quản dữ liệu quyết định việc chuyển dữ liệu cốt lõi ra nước ngoài, xử lý dữ liệu xuyên biên giới.

6. Trường hợp cần chuyển, xử lý xuyên biên giới là dữ liệu quan trọng:

Bên chuyển dữ liệu phải lập hồ sơ đánh giá tác động trước khi chuyển, xử lý dữ liệu xuyên biên giới để phục vụ hoạt động kiểm tra, đánh giá của Bộ Công an hoặc Bộ Quốc phòng trong trường hợp cần thiết (không cần sự chấp thuận của cơ quan có thẩm quyền trước khi thực hiện).

Bên chuyển dữ liệu gửi 01 bản chính hồ sơ tới Bộ Công an hoặc Bộ Quốc phòng theo mẫu ban hành kèm theo Nghị định này trước 15 ngày khi tiến hành xử lý dữ liệu.

7. Việc đánh giá tác động của cơ quan có thẩm quyền tập trung vào việc đánh giá các rủi ro mà hoạt động chuyển, xử lý dữ liệu xuyên biên giới có thể gây ra cho an ninh quốc gia, lợi ích công cộng hoặc quyền và lợi ích hợp pháp của cá nhân, tổ chức, chủ yếu bao gồm các vấn đề sau:

a) Tính hợp pháp, sự cần thiết của mục đích, phạm vi và phương pháp chuyển dữ liệu, xử lý dữ liệu;

b) Tác động của các chính sách và quy định bảo vệ an toàn dữ liệu và môi trường an ninh mạng của quốc gia hoặc khu vực của bên nhận dữ liệu đối với tính bảo mật của dữ liệu; mức độ bảo vệ dữ liệu của bên nhận dữ liệu so với các tiêu chuẩn, quy chuẩn kỹ thuật Việt Nam áp dụng;

c) Quy mô, phạm vi, loại dữ liệu, nguy cơ bị giả mạo, phá hủy, rò rỉ, mất, chuyển giao hoặc sử dụng bất hợp pháp sau khi chuyển giao;

d) Trách nhiệm và nghĩa vụ của các bên có liên quan;

đ) Các vấn đề khác có tác động tới quốc phòng, an ninh, bảo vệ lợi ích quốc gia, lợi ích công cộng, quyền và lợi ích hợp pháp của chủ thể dữ liệu, chủ sở hữu dữ liệu theo quy định của pháp luật Việt Nam và các điều ước quốc tế mà nước Cộng hòa xã hội chủ nghĩa Việt Nam là thành viên.

8. Các trường hợp bên chuyển dữ liệu phải thực hiện sửa đổi, bổ sung hồ sơ đánh giá tác động chuyển, xử lý dữ liệu xuyên biên giới gồm:

a) Khi có sự thay đổi về mục đích, phương pháp, phạm vi, loại dữ liệu chuyển, xử lý, thay đổi mục đích hoặc phương pháp xử lý dữ liệu của bên nhận dữ liệu, ảnh hưởng đến an ninh an toàn dữ liệu; kéo dài thời gian lưu trữ dữ liệu cốt lõi, dữ liệu quan trọng;

b) Thay đổi chính sách, quy định bảo vệ dữ liệu và môi trường an ninh mạng ở quốc gia hoặc khu vực nơi bên nhận dữ liệu, thay đổi quyền kiểm soát thực tế của bên chuyển dữ liệu hoặc bên nhận dữ liệu và các tác động khác đến tính bảo mật của dữ liệu được chuyển.

9. Bộ Quốc phòng, Bộ Công an quyết định yêu cầu bên chuyển dữ liệu ngừng hoạt động chuyển, xử lý dữ liệu cốt lõi, dữ liệu quan trọng trong trường hợp:

a) Dữ liệu cốt lõi, dữ liệu quan trọng đã được chuyển, xử lý xuyên biên giới được sử dụng vào các hoạt động xâm phạm quốc phòng, an ninh, lợi ích quốc gia, lợi ích công cộng, quyền và lợi ích hợp pháp của chủ thể dữ liệu, chủ sở hữu dữ liệu theo quy định của pháp luật Việt Nam và các điều ước quốc tế mà nước Cộng hòa xã hội chủ nghĩa Việt Nam là thành viên.

b) Bên chuyển dữ liệu không chấp hành quy định tại Điều này;

c) Có hành vi vi phạm các quy định về bảo vệ dữ liệu.

10. Việc định lượng dữ liệu cốt lõi, dữ liệu quan trọng khi chuyển, xử lý dữ liệu xuyên biên giới được xác định dựa trên kết quả tích lũy lượng dữ liệu đã được chuyển, xử lý dữ liệu xuyên biên giới, mốc thời gian tính từ ngày 01 tháng 7 năm 2025 đến thời điểm chuyển, xử lý dữ liệu.

11. Trường hợp chuyển, xử lý dữ liệu cốt lõi xuyên biên giới không cần sự chấp thuận của cơ quan có thẩm quyền tại khoản 5 Điều này và trường hợp chuyển, xử lý dữ liệu quan trọng không phải thông báo cho cơ quan có thẩm quyền theo quy định tại khoản 6 Điều này gồm:

a) Trong các tình huống khẩn cấp, thực sự cần thiết phải cung cấp dữ liệu cá nhân ra nước ngoài 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;

b) Thực hiện 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;

c) Trường hợp thực sự cần thiết phải cung cấp dữ liệu nhằm mục đích ký kết hoặc thực hiện hợp đồng, bao gồm trường hợp hợp đồng liên quan đến vận chuyển xuyên biên giới, hậu cần, chuyển tiền, thanh toán, mở tài khoản ngân hàng và khách sạn, xin thị thực, dịch vụ kiểm tra.

12. Trường hợp chuyển, xử lý dữ liệu cốt lõi, dữ liệu quan trọng theo quy định của khoản 11 Điều này phải gửi đánh giá tác động về Bộ Công an (hoặc Bộ Quốc phòng đối với dữ liệu do Bộ Quốc phòng quản lý) theo quy định tại khoản 4 Điều này sau 15 ngày kể từ ngày tiến hành thực hiện.

Điều 13. Các hoạt động khác trong xử lý dữ liệu

1. Thu hồi, xóa, hủy dữ liệu

a) Thu hồi dữ liệu là việc yêu cầu chuyển giao lại dữ liệu và thực hiện xóa, hủy dữ liệu đã cung cấp hoặc yêu cầu ngừng xử lý, sử dụng dữ liệu trong trường hợp không thể xóa, hủy dữ liệu.

Xóa dữ liệu là hoạt động loại bỏ dữ liệu khỏi cấu trúc, môi trường đang được lưu trữ.

Hủy dữ liệu là hoạt động loại bỏ dữ liệu khỏi cấu trúc, môi trường đang được lưu trữ và bảo đảm loại bỏ khả năng phục hồi bằng phương thức ghi đè

hoặc phá huỷ vật lý.

b) Việc xóa, hủy dữ liệu được thực hiện trong 72 giờ sau khi có yêu cầu của chủ thể dữ liệu và phải thông báo kết quả xử lý thu hồi, xóa, hủy dữ liệu cho chủ sở hữu dữ liệu, trừ trường hợp pháp luật có quy định khác. Trường hợp không thể xóa, hủy dữ liệu, chủ sở hữu dữ liệu, chủ quản dữ liệu phải ngừng xử lý, sử dụng dữ liệu.

2. Điều chỉnh, cập nhật dữ liệu là việc thực hiện bổ sung, sửa một hoặc nhiều bản ghi dữ liệu trong cơ sở dữ liệu, hệ thống thông tin.

Chương III **QUẢN TRỊ, QUẢN LÝ, BẢO VỆ DỮ LIỆU**

Điều 14. Quản trị, quản lý dữ liệu

1. Bộ Công an ban hành Khung quản trị, quản lý dữ liệu tổng thể để áp dụng chung cho cơ quan nhà nước có kết nối, chia sẻ dữ liệu với Trung tâm dữ liệu quốc gia.

2. Cơ quan quản lý cơ sở dữ liệu có kết nối, chia sẻ dữ liệu với Trung tâm dữ liệu quốc gia xây dựng Khung quản trị, quản lý dữ liệu chi tiết áp dụng đối với cơ sở dữ liệu do mình quản lý, bảo đảm phù hợp với Khung quản trị, quản lý dữ liệu tổng thể do Bộ Công an ban hành.

3. Cơ quan quản lý cơ sở dữ liệu xây dựng Khung quản trị, quản lý dữ liệu chi tiết bao gồm các nội dung chính sau:

- a) Cơ chế quản lý dữ liệu chủ, bảng mã danh mục dùng chung;
- b) Cơ chế quản lý hoạt động xử lý dữ liệu; phương án mở rộng, dự phòng lưu trữ dữ liệu;
- c) Đánh giá chất lượng dữ liệu; việc áp dụng tiêu chuẩn, quy chuẩn kỹ thuật về chất lượng dữ liệu, kết nối, chia sẻ dữ liệu;
- d) Cơ chế quản lý thông tin đặc tả dữ liệu (siêu dữ liệu);
- đ) Kiến trúc dữ liệu, mô hình dữ liệu;
- e) Cơ chế kết nối, chia sẻ;
- g) Cơ chế bảo vệ dữ liệu;
- h) Cơ chế phát triển, khai thác, sử dụng dữ liệu;
- i) Cơ chế triển khai, kiểm soát, giám sát.

4. Quản lý dữ liệu chủ và dữ liệu danh mục dùng chung

a) Cơ quan quản lý cơ sở dữ liệu ban hành danh mục dữ liệu chủ, dữ liệu danh mục dùng chung trên cơ sở phối hợp, thống nhất với Bộ Công an;

b) Các nội dung quản trị, quản lý dữ liệu chủ bao gồm nguyên tắc cấp mã định danh; các thông tin cơ bản để mô tả, định danh, phân biệt đối tượng cụ thể trong dữ liệu chủ; quy trình tạo lập, cập nhật dữ liệu chủ; lựa chọn công nghệ, công cụ nhằm bảo đảm dữ liệu chủ được thu thập, cập nhật, khai thác và sử dụng chính xác, nhất quán và đầy đủ; thực hiện tạo lập, cập nhật, quản lý dữ liệu chủ; kết nối, chia sẻ dữ liệu chủ vào Cơ sở dữ liệu tổng hợp quốc gia; phối hợp với Bộ Công an để giám sát, đối soát bảo đảm chất lượng dữ liệu chủ trên toàn hệ thống;

c) Dữ liệu chủ trong cơ sở dữ liệu quốc gia, cơ sở dữ liệu khác của cơ quan được giao trách nhiệm tạo lập và quản lý dữ liệu chủ có giá trị sử dụng chính thức, tương đương văn bản giấy được cơ quan có thẩm quyền cung cấp;

d) Bộ Công an xây dựng chính sách quản lý dữ liệu chủ được đồng bộ vào Cơ sở dữ liệu tổng hợp quốc gia; xây dựng các quy trình cho việc thu thập, cập nhật, xóa, sử dụng, chia sẻ, điều phối dữ liệu chủ trong Cơ sở dữ liệu tổng hợp quốc gia; xác định rõ các vai trò trách nhiệm cho chất lượng và tính toàn vẹn của dữ liệu chủ; giám sát chất lượng dữ liệu chủ.

5. Cơ quan nhà nước thực hiện dự án công nghệ thông tin về cơ sở dữ liệu quốc gia, cơ sở dữ liệu chuyên ngành phải lấy ý kiến của Bộ Công an (Trung tâm dữ liệu quốc gia) về nội dung xây dựng, phát triển, bảo vệ, quản trị, xử lý, sử dụng dữ liệu để tránh lãng phí, bảo đảm thống nhất, đồng bộ trong triển khai thực hiện.

Điều 15. Xác định và quản lý rủi ro phát sinh trong xử lý dữ liệu

1. Các loại rủi ro phát sinh trong xử lý dữ liệu bao gồm:

a) Rủi ro quyền riêng tư xảy ra do không tuân thủ quy định của pháp luật về quyền riêng tư của chủ thể dữ liệu trong quá trình xử lý và chuyển dữ liệu;

b) Rủi ro an ninh mạng xảy ra do không áp dụng các biện pháp cần thiết để bảo vệ dữ liệu không được công khai khỏi những truy cập trái phép từ các đối tượng bên ngoài hoặc dữ liệu bị rò rỉ ra bên ngoài;

c) Rủi ro nhận dạng và quản lý truy cập xảy ra do không bảo đảm việc bảo vệ dữ liệu không được công khai khỏi những truy cập trái phép;

d) Rủi ro khác trong xử lý dữ liệu bao gồm: rủi ro chia sẻ dữ liệu xảy ra khi không có khả năng duy trì quyền kiểm soát đối với dữ liệu đã chia sẻ; rủi ro quản lý dữ liệu xảy ra do chất lượng của dữ liệu không đảm bảo.

2. Một số biện pháp phòng ngừa rủi ro phát sinh trong xử lý dữ liệu bao gồm:

a) Thực hiện sao lưu dữ liệu thường xuyên và bảo đảm an toàn;

b) Định kỳ bảo trì, bảo dưỡng, nâng cấp hệ thống nhằm duy trì và cải thiện hiệu suất, tính năng, tính bảo mật và tính nhất quán của hệ thống cơ sở dữ liệu;

có biện pháp ứng phó khôi phục hệ thống để bảo đảm tính liên tục của hệ thống;

c) Thực hiện các biện pháp bảo vệ dữ liệu theo quy định;

d) Phân cấp chặt chẽ quyền truy cập đối với từng loại dữ liệu để phòng ngừa việc truy cập dữ liệu trái phép;

đ) Sử dụng các hệ thống giám sát và phát hiện xâm nhập để theo dõi hoạt động mạng và phát hiện các hành vi bất thường hoặc truy cập trái phép;

e) Cài đặt và duy trì các phần mềm bảo mật;

g) Thực hiện đánh giá rủi ro định kỳ hàng năm để xác định các lỗ hổng trong hệ thống và áp dụng các biện pháp phòng ngừa rủi ro tương ứng;

h) Xây dựng phương án, kế hoạch xử lý sự cố để chủ động, kịp thời ứng phó, khắc phục sự cố;

i) Đào tạo, bồi dưỡng, tập huấn kỹ năng bảo vệ dữ liệu, cách nhận biết các mối đe dọa, cách xử lý khi phát hiện rủi ro bảo mật; thường xuyên diễn tập phòng ngừa sự cố, giám sát, phát hiện, bảo đảm kịp thời ứng phó, khắc phục sự cố;

k) Các biện pháp khác theo quy định pháp luật.

Điều 16. Bảo vệ dữ liệu

1. Cơ quan nhà nước có trách nhiệm tổ chức quản lý và bảo vệ dữ liệu thuộc phạm vi quản lý, bao gồm thiết lập hệ thống quản lý, giám sát, đánh giá rủi ro và cảnh báo sớm trong toàn bộ quá trình xử lý dữ liệu; thực hiện phân cấp, phân quyền truy cập phù hợp đối với các loại dữ liệu khác nhau, bảo đảm tuân thủ các chính sách chung về bảo vệ dữ liệu.

Khuyến khích các chủ quản dữ liệu không thuộc cơ quan nhà nước xây dựng các quy định riêng về bảo vệ dữ liệu do mình quản lý.

2. Việc bảo vệ dữ liệu cốt lõi, dữ liệu quan trọng là dữ liệu cá nhân thực hiện theo quy định của Luật Dữ liệu và Nghị định này.

Trường hợp chuyên, xử lý dữ liệu cốt lõi, dữ liệu quan trọng xuyên biên giới và quản lý, bảo vệ dữ liệu cốt lõi, dữ liệu quan trọng là dữ liệu cá nhân thực hiện theo quy định của Điều 12 và khoản 11 Điều 17 Nghị định này; không phải đánh giá tác động theo pháp luật về bảo vệ dữ liệu cá nhân.

3. Chủ quản dữ liệu cung cấp hoặc ủy thác việc xử lý dữ liệu cốt lõi, dữ liệu quan trọng cho tổ chức, cá nhân không thuộc quy định tại Điều 12 Nghị định này phải đáp ứng những yêu cầu như sau:

a) Thỏa thuận với bên nhận dữ liệu về mục đích, phương thức, phạm vi, nghĩa vụ bảo vệ an ninh thông qua hợp đồng và tiến hành giám sát việc thực hiện nghĩa vụ của bên nhận dữ liệu. Hồ sơ về việc xử lý dữ liệu quan trọng

được cung cấp hoặc ủy thác cho các bên nhận dữ liệu khác phải được lưu trữ ít nhất 3 năm;

b) Khi thực hiện cung cấp, ủy thác xử lý dữ liệu cốt lõi, dữ liệu quan trọng, chủ quản dữ liệu cần thực hiện mã hóa, ký số và thực hiện các biện pháp bảo mật khác để bảo đảm tính bí mật, toàn vẹn và tính chống chối bỏ;

c) Bên tiếp nhận dữ liệu cốt lõi, dữ liệu quan trọng phải thực hiện nghĩa vụ bảo vệ dữ liệu, xử lý dữ liệu cốt lõi, dữ liệu quan trọng theo đúng mục đích, phương thức, phạm vi đã thỏa thuận.

4. Các biện pháp bảo vệ dữ liệu bao gồm:

a) Quản lý có liên quan đến xử lý dữ liệu gồm: xây dựng chính sách, quy chế, tiêu chí đánh giá an toàn, an ninh dữ liệu để bảo đảm tuân thủ các tiêu chuẩn, quy chuẩn kỹ thuật, quy định về bảo vệ dữ liệu và các biện pháp quản lý khác theo quy định của pháp luật;

b) Biện pháp kỹ thuật có liên quan đến xử lý dữ liệu: bảo đảm an ninh vật lý, kiểm soát truy cập, kiểm tra an ninh mạng và các biện pháp kỹ thuật khác theo quy định của pháp luật;

c) Quản lý nhân lực bảo vệ dữ liệu: xây dựng quy chế quản lý con người, đào tạo nhân lực bảo vệ dữ liệu;

d) Các biện pháp bảo vệ dữ liệu khác theo quy định pháp luật.

Điều 17. Quản lý bảo vệ dữ liệu trong quá trình xử lý

1. Chủ quản dữ liệu phải thiết lập hệ thống quản lý việc bảo vệ dữ liệu trong toàn bộ quá trình xử lý dữ liệu.

2. Chủ quản dữ liệu thực hiện các biện pháp bảo vệ dữ liệu trong quá trình thu thập, tạo lập dữ liệu. Đối với dữ liệu cốt lõi, dữ liệu quan trọng chủ quản dữ liệu cần thực hiện các nội dung sau:

a) Xây dựng quy trình thu thập, tạo lập dữ liệu và đánh giá, áp dụng các biện pháp bảo vệ trước khi thu thập, tạo lập dữ liệu;

b) Kiểm tra tính xác thực, giám sát chất lượng dữ liệu và truy xuất nguồn gốc dữ liệu.

3. Chủ quản dữ liệu thực hiện lưu trữ dữ liệu theo phương pháp, thời hạn theo quy định của pháp luật. Đối với dữ liệu cốt lõi, dữ liệu quan trọng, chủ quản dữ liệu thực hiện các nội dung sau:

a) Xây dựng quy trình lưu trữ dữ liệu, trong đó quy định về quy trình sao lưu, phục hồi dữ liệu, ghi nhật ký lưu trữ, sao lưu, phục hồi dữ liệu;

b) Xây dựng hệ thống quản lý lưu trữ dữ liệu và áp dụng các công cụ, biện pháp kỹ thuật để bảo vệ dữ liệu trong quá trình lưu trữ, tự động thực hiện việc sao lưu, phục hồi dữ liệu;

c) Thực hiện xóa, hủy dữ liệu khi hết thời hạn lưu trữ hoặc dữ liệu không còn cần thiết cho mục đích xử lý.

4. Khi xử lý, sử dụng dữ liệu cốt lõi, dữ liệu quan trọng, chủ quản dữ liệu cần thực hiện:

a) Xây dựng, triển khai quy chế truy cập, truy xuất dữ liệu bảo đảm tuân thủ các nguyên tắc đặc quyền tối thiểu trong quá trình xử lý, sử dụng dữ liệu;

b) Xây dựng hệ thống kiểm soát truy cập dữ liệu, trong đó thiết lập nền tảng quản lý truy cập và nhận dạng thống nhất; áp dụng các biện pháp kỹ thuật để bảo vệ dữ liệu, kiểm soát việc truy cập, truy xuất dữ liệu trong quá trình xử lý, sử dụng dữ liệu.

5. Chủ quản dữ liệu có trách nhiệm làm rõ phạm vi, mục đích, quy trình, xây dựng quy chế bảo vệ và áp dụng các biện pháp bảo vệ dựa trên phân loại, mức độ và mục đích, trường hợp ứng dụng của dữ liệu được cung cấp ra bên ngoài.

6. Chủ sở hữu dữ liệu phải phân tích, đánh giá tác động đến quốc phòng, an ninh, đối ngoại, kinh tế vĩ mô, ổn định xã hội, sức khỏe và an toàn cộng đồng trước khi công khai dữ liệu.

7. Chủ sở hữu dữ liệu, chủ quản dữ liệu xây dựng phương án xóa, hủy dữ liệu, làm rõ mục tiêu, quy tắc, quy trình, kỹ thuật xóa, hủy, ghi nhận và lưu giữ hoạt động xóa, hủy. Trường hợp xóa, hủy dữ liệu quan trọng, dữ liệu cốt lõi thì chủ quản dữ liệu phải có tài liệu chứng minh hoạt động xóa, hủy dữ liệu bảo đảm không thể khôi phục.

8. Trường hợp chủ quản dữ liệu có nhu cầu chuyển dữ liệu vì tổ chức lại, giải thể, phá sản thì phải làm rõ kế hoạch chuyển dữ liệu và thông báo cho cơ quan, tổ chức, cá nhân bị ảnh hưởng.

Trường hợp tổ chức lại, giải thể tổ chức có quản lý dữ liệu cốt lõi, dữ liệu quan trọng, chủ quản dữ liệu phải áp dụng các biện pháp bảo đảm an toàn dữ liệu, báo cáo phương án xử lý dữ liệu, tên hoặc thông tin của bên tiếp nhận cho cơ quan có thẩm quyền có liên quan.

9. Trường hợp chủ quản dữ liệu ủy thác cho tổ chức, cá nhân khác thực hiện hoạt động xử lý dữ liệu thì phải làm rõ trách nhiệm, nghĩa vụ bảo mật dữ liệu của bên ủy thác và bên được ủy thác thông qua hợp đồng, thỏa thuận ủy thác. Trường hợp ủy thác xử lý dữ liệu quan trọng, dữ liệu cốt lõi thì bên ủy thác phải xác minh năng lực, trình độ bảo vệ dữ liệu của bên được ủy thác.

10. Chủ quản dữ liệu cốt lõi, dữ liệu quan trọng phải ghi nhật ký xử lý dữ liệu trong toàn bộ quá trình xử lý dữ liệu. Nhật ký được lưu giữ trong thời gian ít nhất sáu tháng.

11. Chủ quản dữ liệu cốt lõi, dữ liệu quan trọng hàng năm phải thực hiện đánh giá rủi ro đối với hoạt động xử lý dữ liệu cốt lõi, dữ liệu quan trọng trong phạm vi quản lý, lập, lưu trữ Báo cáo đánh giá rủi ro theo mẫu ban hành kèm theo Nghị định này và phải luôn có sẵn để phục vụ hoạt động kiểm tra, đánh giá của cơ quan có thẩm quyền, trừ trường hợp đã lập Hồ sơ đánh giá tác động chuyển, xử lý dữ liệu xuyên biên giới theo quy định tại Điều 12 Nghị định này. Báo cáo đánh giá rủi ro bao gồm:

a) Thông tin cơ bản về chủ quản dữ liệu, thông tin về bộ phận có chức năng bảo vệ an toàn dữ liệu, tên và thông tin liên lạc của người chịu trách nhiệm về bảo vệ dữ liệu;

b) Mục đích, loại, số lượng, phương pháp, phạm vi, thời gian lưu trữ, vị trí lưu trữ dữ liệu, hoạt động xử lý dữ liệu và hoàn cảnh thực hiện các hoạt động xử lý dữ liệu;

c) Hệ thống quản lý bảo vệ dữ liệu, các biện pháp kỹ thuật mã hóa, sao lưu, dán nhãn, kiểm soát truy cập và xác thực, các biện pháp cần thiết khác;

d) Rủi ro an toàn dữ liệu đã phát hiện, sự cố an toàn dữ liệu đã xảy ra và cách giải quyết;

đ) Các nội dung báo cáo khác theo quy định của các cơ quan có thẩm quyền có liên quan.

Điều 18. Quản lý nhân sự và đào tạo, bồi dưỡng nhân sự bảo vệ dữ liệu

1. Chủ sở hữu dữ liệu, chủ quản dữ liệu cốt lõi, dữ liệu quan trọng phải xác định người chịu trách nhiệm về bảo vệ dữ liệu và bộ phận bảo vệ an toàn dữ liệu.

2. Người chịu trách nhiệm về bảo vệ dữ liệu có chức năng, nhiệm vụ quản lý, bảo vệ dữ liệu cốt lõi, dữ liệu quan trọng bao gồm tổ chức xây dựng các kế hoạch bảo vệ an toàn dữ liệu quan trọng, tổ chức đánh giá rủi ro; thực hiện báo cáo trực tiếp về tình hình bảo vệ dữ liệu cho các cơ quan có thẩm quyền theo quy định; phải được đào tạo, bồi dưỡng kiến thức về bảo vệ dữ liệu.

3. Bộ phận bảo vệ an toàn dữ liệu có chức năng, nhiệm vụ như sau:

a) Phát triển, triển khai hệ thống quản lý bảo vệ dữ liệu, quy trình vận hành, kế hoạch ứng cứu khẩn cấp sự cố bảo vệ dữ liệu;

b) Định kỳ tổ chức và thực hiện các hoạt động như giám sát rủi ro an toàn dữ liệu, đánh giá rủi ro, diễn tập khẩn cấp, tuyên truyền, giáo dục, đào tạo, giải quyết kịp thời các rủi ro, sự cố an toàn dữ liệu mạng;

c) Nghiên cứu và đề xuất các quyết định liên quan đến bảo vệ dữ liệu cốt lõi, dữ liệu quan trọng;

d) Tiếp nhận và xử lý các báo cáo về bảo vệ dữ liệu của đơn vị.

4. Chủ sở hữu dữ liệu, chủ quản dữ liệu cốt lõi, dữ liệu quan trọng phải thực hiện:

a) Làm rõ các yêu cầu quản lý an toàn trong tuyển dụng, sử dụng, đào tạo, giới thiệu, luân chuyển, từ chức, đánh giá và lựa chọn nhân sự;

b) Không bố trí những người có tiền án trong lĩnh vực công nghệ thông tin, mạng viễn thông làm người chịu trách nhiệm về bảo vệ dữ liệu;

c) Ký thỏa thuận trách nhiệm bảo mật với nhân viên xử lý dữ liệu.

5. Xây dựng kế hoạch và thực hiện đào tạo về bảo vệ dữ liệu hàng năm.

6. Người chịu trách nhiệm về bảo vệ dữ liệu được thỏa thuận với chủ sở hữu, chủ quản dữ liệu về các trường hợp miễn trừ trách nhiệm khi xảy ra thiệt hại đối với dữ liệu được bảo vệ.

Điều 19. Giám sát bảo mật dữ liệu, cảnh báo sớm và quản lý khẩn cấp

1. Nội dung giám sát bảo mật dữ liệu, cảnh báo sớm và quản lý khẩn cấp gồm:

a) Thiết lập cơ chế giám sát rủi ro an toàn dữ liệu;

b) Tổ chức soạn thảo các giao diện, tiêu chuẩn giám sát;

c) Xây dựng cơ chế báo cáo, chia sẻ thông tin rủi ro an toàn dữ liệu, thống nhất thu thập, phân tích, đánh giá, báo cáo thông tin rủi ro an toàn dữ liệu;

d) Xây dựng kế hoạch ứng phó khẩn cấp sự cố an toàn dữ liệu.

2. Bộ Công an thực hiện giám sát bảo mật, cảnh báo sớm và quản lý khẩn cấp dữ liệu trừ nội dung quy định tại khoản 3 Điều này.

3. Bộ Quốc phòng thực hiện giám sát bảo mật, cảnh báo sớm và quản lý khẩn cấp đối với các dữ liệu thuộc phạm vi quản lý.

4. Chủ quản dữ liệu có trách nhiệm:

a) Thông báo kịp thời cho chủ sở hữu dữ liệu về các sự cố an toàn dữ liệu có thể gây tổn hại đến quyền và lợi ích hợp pháp của cá nhân, tổ chức và đưa ra các biện pháp giảm thiểu thiệt hại;

b) Sau khi xảy ra sự cố an toàn dữ liệu, phải kịp thời tiến hành ứng phó khẩn cấp theo kế hoạch ứng phó khẩn cấp, báo cáo các sự cố bảo mật liên quan đến dữ liệu quan trọng và dữ liệu cốt lõi cho Bộ Công an, Bộ Quốc phòng quản lý trong thời gian sớm nhất có thể.

5. Bộ Công an thiết lập cơ chế giám sát rủi ro an toàn dữ liệu, xây dựng các tiêu chuẩn giám sát và cảnh báo sớm an toàn dữ liệu, phối hợp xây dựng

các phương tiện kỹ thuật giám sát và cảnh báo sớm an toàn dữ liệu, hình thành năng lực giám sát, cảnh báo sớm, xử lý, truy xuất nguồn gốc, tăng cường chia sẻ thông tin với các bộ phận liên quan.

Chủ quản dữ liệu phải thực hiện giám sát rủi ro an toàn dữ liệu, kịp thời điều tra các rủi ro an ninh tiềm ẩn và áp dụng các biện pháp cần thiết để ngăn ngừa rủi ro an toàn dữ liệu.

6. Bộ Công an xây dựng cơ chế báo cáo, chia sẻ thông tin rủi ro an toàn dữ liệu, thống nhất thu thập, phân tích, đánh giá, báo cáo thông tin rủi ro an toàn dữ liệu, khuyến khích các tổ chức cung cấp dịch vụ bảo mật, tổ chức nghiên cứu khoa học chia sẻ thông tin về rủi ro an toàn dữ liệu.

Chủ quản dữ liệu tóm tắt và phân tích riêng các rủi ro bảo mật dữ liệu trong phạm vi quản lý, đồng thời báo cáo kịp thời các rủi ro có thể gây ra các sự cố bảo mật lớn về Bộ Công an.

7. Bộ Công an xây dựng kế hoạch ứng phó khẩn cấp sự cố an toàn dữ liệu, bao gồm cơ cấu và trách nhiệm tổ chức khẩn cấp, phân loại và phân cấp các sự cố an toàn dữ liệu, giám sát và cảnh báo sớm, quy trình ứng phó khẩn cấp, các biện pháp bảo vệ, đồng thời tổ chức, phối hợp ứng phó với các sự cố dữ liệu quan trọng, an toàn dữ liệu cốt lõi.

8. Chủ quản dữ liệu thực hiện diễn tập kế hoạch dự phòng đối với các sự cố an toàn dữ liệu quan trọng, cốt lõi tiến hành diễn tập khẩn cấp định kỳ 06 tháng/lần, lưu hồ sơ diễn tập và báo cáo tóm tắt diễn tập, cập nhật kịp thời các kế hoạch dự phòng theo những thay đổi lớn trong chính hệ thống xử lý dữ liệu hoặc môi trường bên ngoài.

Chương IV

TRUNG TÂM DỮ LIỆU QUỐC GIA, CƠ SỞ DỮ LIỆU TỔNG HỢP QUỐC GIA

Điều 20. Cơ sở hạ tầng của Trung tâm dữ liệu quốc gia

1. Hệ thống thông tin của Trung tâm dữ liệu quốc gia tách biệt với hệ thống phát triển, kiểm tra và thử nghiệm; bảo đảm an ninh, bảo mật theo cấp độ nhằm kiểm soát, phát hiện, ngăn chặn các nguy cơ mất an ninh, an toàn thông tin.

2. Trung tâm dữ liệu quốc gia xây dựng, phát triển cơ sở hạ tầng điện toán đám mây và triển khai thành các vùng chức năng để phục vụ nhu cầu của cơ quan nhà nước bảo đảm việc phát triển các phân hệ tích hợp, đồng bộ, khai thác dữ liệu, yêu cầu cao về bảo mật thông tin.

3. Trung tâm dữ liệu quốc gia thiết lập hạ tầng tính toán hiệu suất cao và hệ thống phân tích dữ liệu phục vụ công tác quản lý với các mô hình phân tích dự báo phục vụ công tác khai thác từ Cơ sở dữ liệu tổng hợp quốc gia. Cung

cấp điều kiện kỹ thuật hỗ trợ việc nghiên cứu phát triển lĩnh vực toán ứng dụng; hỗ trợ công tác xây dựng các cơ chế chính sách, quy hoạch, chiến lược phát triển quốc gia, phát triển sản phẩm, dịch vụ về dữ liệu phục vụ phát triển kinh tế - xã hội.

4. Trung tâm dữ liệu quốc gia thiết lập Cổng dữ liệu quốc gia là đầu mối để các cơ quan nhà nước công bố thông tin về các loại dữ liệu đang quản lý; công bố dữ liệu mở, cung cấp dữ liệu mở nhằm tăng cường tính minh bạch trong hoạt động của Chính phủ và thúc đẩy sáng tạo, phát triển kinh tế, xã hội; để tổ chức, cá nhân cung cấp dữ liệu phục vụ cho các mục tiêu vì lợi ích chung, cải thiện việc cung cấp dịch vụ công, hoạch định chính sách công hoặc mục đích nghiên cứu khoa học vì lợi ích chung; phục vụ cơ quan, tổ chức, cá nhân truy cập, tìm kiếm, khám phá và sử dụng dữ liệu mở.

5. Trung tâm dữ liệu quốc gia xây dựng ứng dụng trên thiết bị số phục vụ khai thác, sử dụng dữ liệu của Trung tâm dữ liệu quốc gia, cung cấp các sản phẩm, dịch vụ về dữ liệu và phát triển các tiện ích khác để phục vụ cơ quan, tổ chức, cá nhân.

6. Trung tâm dữ liệu quốc gia xây dựng Hệ thống liên lạc với cá nhân và tổ chức phục vụ hoạt động của Trung tâm dữ liệu quốc gia.

7. Trung tâm dữ liệu quốc gia cung cấp các loại dịch vụ sau:

a) Dịch vụ hạ tầng nhà trạm, chỗ đặt máy chủ, cung cấp không gian hạ tầng chỗ đặt, hệ thống điện, điều hòa và các thiết bị liên quan khác để triển khai hệ thống thông tin cơ sở dữ liệu, cho phép chủ quản cơ sở dữ liệu, cơ quan, tổ chức có nhu cầu chủ động sử dụng, kiểm soát hệ thống của mình, theo hình thức sử dụng không gian chung hoặc theo khu riêng, tuân thủ quy định về quản lý, vận hành Trung tâm dữ liệu quốc gia;

b) Dịch vụ cung cấp máy chủ, thiết bị mạng, an toàn thông tin mạng, an ninh mạng, bảo mật hoặc lưu trữ với cấu hình đa dạng, không gian chỗ đặt tương ứng tại các Trung tâm dữ liệu quốc gia, phù hợp với nhu cầu của chủ quản cơ sở dữ liệu, cơ quan, tổ chức có nhu cầu;

c) Dịch vụ triển khai và vận hành hạ tầng kỹ thuật phục vụ cơ sở dữ liệu quốc gia và hệ thống thông tin cơ sở dữ liệu, cơ sở dữ liệu và hệ thống thông tin khác.

8. Cơ quan nhà nước, tổ chức chính trị - xã hội xác định loại dịch vụ cung cấp bởi Trung tâm dữ liệu quốc gia theo quy định tại khoản 7 Điều này, bảo đảm phù hợp với hiện trạng, yêu cầu nghiệp vụ, quy định về đầu tư dự án công nghệ thông tin sử dụng vốn ngân sách nhà nước và gửi văn bản đề nghị Trung tâm dữ liệu quốc gia cung cấp dịch vụ. Nội dung văn bản đề nghị cần xác định rõ nhu cầu sử dụng dịch vụ của Trung tâm dữ liệu quốc gia; quy mô hệ thống dự kiến đặt tại Trung tâm dữ liệu quốc gia; nhu cầu về nhân lực hỗ trợ quản trị,

vận hành hạ tầng, hệ thống thông tin.

9. Bộ trưởng Bộ Công an hướng dẫn việc cung cấp, triển khai các dịch vụ của Trung tâm dữ liệu quốc gia khi có đủ các điều kiện về hạ tầng.

Điều 21. Trách nhiệm của Trung tâm dữ liệu quốc gia

1. Hướng dẫn cơ quan, tổ chức, cá nhân trong việc áp dụng tiêu chuẩn, quy chuẩn kỹ thuật về dữ liệu thuộc phạm vi đồng bộ về Trung tâm dữ liệu quốc gia.

2. Thực hiện các biện pháp giám sát, đánh giá chất lượng dữ liệu được chia sẻ, đồng bộ về Trung tâm dữ liệu quốc gia.

3. Điều phối dữ liệu của Cơ sở dữ liệu tổng hợp quốc gia.

4. Thực hiện các biện pháp bảo vệ dữ liệu được áp dụng ngay từ khi bắt đầu và trong suốt quá trình xử lý dữ liệu theo quy định tại khoản 6 Điều 16 Nghị định này.

5. Thực hiện ký kết các thoả thuận, biên bản ghi nhớ với các cơ quan, tổ chức quốc tế để thúc đẩy hợp tác quốc tế trong quản lý, bảo vệ dữ liệu, nghiên cứu khoa học, chuyển giao dữ liệu xuyên biên giới, đào tạo, nâng cao năng lực, trình độ về các nội dung liên quan đến dữ liệu nhằm thúc đẩy các hoạt động đổi mới sáng tạo, chuyển giao công nghệ phục vụ phát triển kinh tế - xã hội.

6. Giúp Bộ Công an thực hiện quản lý nhà nước về dữ liệu.

Điều 22. Bảo đảm nguồn lực xây dựng, phát triển Trung tâm dữ liệu quốc gia

1. Trung tâm dữ liệu quốc gia xây dựng kế hoạch, chương trình đào tạo, hợp tác quốc tế, nâng cao chất lượng nguồn nhân lực của Trung tâm dữ liệu quốc gia.

2. Cán bộ, chiến sĩ làm việc tại Trung tâm dữ liệu quốc gia được hưởng mức hỗ trợ là 500.000 đồng/ngày làm việc từ nguồn thu phí khai thác, sử dụng dữ liệu trong Cơ sở dữ liệu tổng hợp quốc gia sau khi nộp vào ngân sách nhà nước.

Tổ chức, đơn vị sự nghiệp công lập trực thuộc Trung tâm dữ liệu quốc gia được vận dụng chế độ hỗ trợ này để quyết định các chế độ đối với người làm công tác chuyên môn về dữ liệu.

3. Bộ trưởng Bộ Công an ban hành danh mục vị trí việc làm tại Trung tâm dữ liệu quốc gia; ban hành cơ chế thu hút, trọng dụng, đãi ngộ nguồn nhân lực chất lượng cao làm việc cho Trung tâm dữ liệu quốc gia.

Điều 23. Khai thác và sử dụng Cơ sở dữ liệu tổng hợp quốc gia

1. Khai thác qua kết nối, chia sẻ trực tiếp thông tin với Cơ sở dữ liệu tổng hợp quốc gia

a) Trung tâm dữ liệu quốc gia cấp tài khoản cho cơ quan, tổ chức để truy cập, khai thác thông tin trong Cơ sở dữ liệu tổng hợp quốc gia;

b) Cơ quan, tổ chức được Trung tâm dữ liệu quốc gia cấp tài khoản có trách nhiệm tạo lập, quản lý tài khoản riêng trên hệ thống thông tin của mình đã kết nối với Cơ sở dữ liệu tổng hợp quốc gia và phân quyền sử dụng tài khoản đã tạo lập cho cá nhân thuộc quyền quản lý theo chức năng, nhiệm vụ được giao;

c) Cá nhân được phân quyền sử dụng tài khoản riêng thuộc cơ quan, tổ chức sử dụng tài khoản riêng đó để tra cứu, khai thác thông tin về công dân trong Cơ sở dữ liệu tổng hợp quốc gia thông qua hệ thống thông tin của cơ quan, tổ chức;

d) Hệ thống thông tin của cơ quan, tổ chức gửi yêu cầu khai thác thông tin tới Cơ sở dữ liệu tổng hợp quốc gia qua tài khoản đã được Trung tâm dữ liệu quốc gia cấp. Kết quả khai thác được thể hiện dưới dạng văn bản giấy hoặc văn bản điện tử và được lưu trữ tại hệ thống thông tin được kết nối, chia sẻ, khai thác thông tin;

đ) Trung tâm dữ liệu quốc gia có trách nhiệm kiểm tra, xác thực thông tin tài khoản và trả kết quả khai thác theo yêu cầu, phù hợp với quyền hạn, phạm vi thông tin được khai thác của tài khoản.

2. Cơ quan, tổ chức, cá nhân thực hiện khai thác thông tin trong Cơ sở dữ liệu tổng hợp quốc gia qua Cổng dữ liệu quốc gia, Cổng Dịch vụ công quốc gia tại Trung tâm dữ liệu quốc gia và thiết bị, phương tiện, phần mềm theo hướng dẫn của Bộ Công an.

3. Cơ quan, tổ chức, cá nhân thực hiện khai thác thông tin trong Cơ sở dữ liệu tổng hợp quốc gia qua cổng thông tin điện tử, hệ thống thông tin giải quyết thủ tục hành chính theo hướng dẫn của bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ, Ủy ban nhân dân tỉnh, thành phố trực thuộc trung ương.

4. Khai thác bằng văn bản yêu cầu khai thác, cung cấp thông tin

a) Cơ quan, tổ chức, cá nhân có văn bản yêu cầu khai thác, cung cấp thông tin trong Cơ sở dữ liệu tổng hợp quốc gia và gửi về Trung tâm dữ liệu quốc gia;

b) Văn bản yêu cầu khai thác, cung cấp thông tin phải nêu rõ mục đích, nội dung, phạm vi thông tin cần khai thác trong Cơ sở dữ liệu tổng hợp quốc gia và cam đoan về việc chịu trách nhiệm trong sử dụng thông tin khi được khai thác và các thông tin khác;

c) Trong thời hạn 03 ngày làm việc, kể từ ngày nhận được văn bản yêu cầu khai thác thông tin trong Cơ sở dữ liệu tổng hợp quốc gia thì người có thẩm quyền xem xét, quyết định cho phép khai thác thông tin;

d) Trường hợp đồng ý cho phép khai thác thông tin thì có văn bản trả lời và cung cấp thông tin cho cơ quan, tổ chức, cá nhân. Trường hợp không đồng ý cho phép khai thác thông tin thì phải có văn bản trả lời và nêu rõ lý do.

5. Cơ sở dữ liệu tổng hợp quốc gia phục vụ thực hiện thủ tục hành chính:

a) Tự động thực hiện thủ tục hành chính, chế độ, chính sách cho cá nhân, tổ chức khi thông tin, dữ liệu phục vụ cho việc xem xét, giải quyết thủ tục hành chính đã có đầy đủ trong Cơ sở dữ liệu tổng hợp quốc gia. Cơ quan, người có thẩm quyền chủ động giải quyết thủ tục hành chính, chế độ, chính sách cho cá nhân, tổ chức dựa trên thông tin, dữ liệu đã được kết nối, chia sẻ, khai thác từ Cơ sở dữ liệu tổng hợp quốc gia và sự đồng ý của cá nhân, tổ chức;

b) Khai thác, tái sử dụng dữ liệu, xây dựng dịch vụ công trực tuyến tập trung trên Cổng dịch vụ công quốc gia, bảo đảm đơn giản, thông suốt, thuận lợi, thân thiện với người sử dụng, tiết kiệm, hiệu quả;

c) Kết nối, chia sẻ dữ liệu giữa Cơ sở dữ liệu tổng hợp quốc gia với Hệ thống thông tin giải quyết thủ tục hành chính cấp bộ, cấp tỉnh phục vụ tiếp nhận, giải quyết thủ tục hành chính cho cá nhân, tổ chức, bảo đảm không yêu cầu cá nhân, tổ chức khai báo, cung cấp lại thông tin, giấy tờ đã có trong Cơ sở dữ liệu tổng hợp quốc gia; đồng bộ đầy đủ dữ liệu số hóa hồ sơ, kết quả giải quyết thủ tục hành chính từ Hệ thống thông tin giải quyết thủ tục hành chính cấp bộ, cấp tỉnh, Cơ sở dữ liệu quốc gia, chuyên ngành do bộ, cơ quan, địa phương quản lý với Cổng Dịch vụ công quốc gia, Cơ sở dữ liệu tổng hợp quốc gia phục vụ khai thác, tái sử dụng dữ liệu, bảo đảm cá nhân, tổ chức chỉ cung cấp thông tin, dữ liệu, giấy tờ một lần cho cơ quan nhà nước trong thực hiện thủ tục hành chính, dịch vụ công.

Điều 24. Kết nối, chia sẻ dữ liệu với Cơ sở dữ liệu tổng hợp quốc gia

1. Chủ quản các cơ sở dữ liệu của các cơ quan nhà nước khi xây dựng cơ sở dữ liệu có kết nối đến Trung tâm dữ liệu quốc gia có trách nhiệm tuân thủ hướng dẫn của Trung tâm dữ liệu quốc gia để bảo đảm việc kết nối, chia sẻ dữ liệu.

2. Trung tâm dữ liệu quốc gia và cơ quan quản lý cơ sở dữ liệu xây dựng thỏa thuận kết nối, chia sẻ dữ liệu như sau bao gồm những nội dung:

- a) Mục đích chia sẻ dữ liệu;
- b) Phạm vi dữ liệu được chia sẻ;
- c) Phương thức kết nối, chia sẻ dữ liệu;
- d) Thời gian, tần suất chia sẻ dữ liệu;
- đ) Các nội dung khác có liên quan.

3. Phương thức chia sẻ dữ liệu

a) Việc chia sẻ dữ liệu giữa cơ sở dữ liệu của cơ quan nhà nước được thực hiện thông qua Nền tảng chia sẻ, điều phối dữ liệu của Trung tâm dữ liệu quốc gia và các nền tảng tích hợp và chia sẻ dữ liệu khác;

b) Việc chia sẻ dữ liệu giữa tổ chức, cá nhân với Cơ sở dữ liệu tổng hợp quốc gia thực hiện qua Nền tảng chia sẻ, điều phối dữ liệu, cổng dữ liệu, qua tập tin và các phương thức khác tùy theo thỏa thuận chia sẻ giữa các bên.

4. Trung tâm dữ liệu quốc gia thực hiện giám sát hoạt động chia sẻ thông qua hệ thống giám sát để có đánh giá việc cung cấp và sử dụng dữ liệu.

Điều 25. Cung cấp dữ liệu cho Cơ sở dữ liệu tổng hợp quốc gia

1. Tổ chức, cá nhân không phải là cơ quan nhà nước cung cấp dữ liệu cho Cơ sở dữ liệu tổng hợp quốc gia thông qua thỏa thuận với Trung tâm dữ liệu quốc gia. Văn bản thỏa thuận cung cấp dữ liệu phải xác định rõ mục đích cung cấp dữ liệu; phạm vi dữ liệu được cung cấp; phương thức cung cấp dữ liệu; thời gian, tần suất cung cấp và các nội dung liên quan khác.

2. Trách nhiệm của cơ quan quản lý cơ sở dữ liệu trong việc cung cấp dữ liệu cho Cơ sở dữ liệu tổng hợp quốc gia

a) Đồng bộ dữ liệu cho Cơ sở dữ liệu tổng hợp quốc gia theo quy định tại khoản 1 Điều 34 Luật Dữ liệu;

b) Đồng bộ dữ liệu chủ, dữ liệu phục vụ giải quyết thủ tục hành chính trên Cổng dịch vụ công quốc gia thuộc phạm vi quản lý ngay khi có sự điều chỉnh, cập nhật vào Cơ sở dữ liệu tổng hợp quốc gia;

c) Đối với dữ liệu khác thực hiện đồng bộ khi có điều chỉnh, cập nhật theo thỏa thuận với Trung tâm dữ liệu quốc gia.

3. Trung tâm dữ liệu quốc gia phối hợp với cơ quan quản lý cơ sở dữ liệu triển khai các biện pháp kỹ thuật phù hợp để bảo đảm khi dữ liệu chủ thay đổi, dữ liệu trong các cơ sở dữ liệu tham chiếu đến phải được đồng bộ tương ứng.

Chương V

TRÁCH NHIỆM CỦA CÁC CƠ QUAN, TỔ CHỨC

Điều 26. Trách nhiệm của Bộ Công an

1. Chủ trì, phối hợp với các cơ quan có liên quan tổ chức triển khai, hướng dẫn, kiểm tra, đôn đốc việc thực hiện Nghị định này.

2. Chủ trì, phối hợp với các cơ quan có liên quan quản lý hoạt động xây dựng, phát triển, bảo vệ, quản trị, xử lý, sử dụng dữ liệu; bảo đảm an ninh dữ liệu, đấu tranh phòng, chống tội phạm và các hành vi vi phạm pháp luật trong lĩnh vực dữ liệu; quản lý, theo dõi, giám sát đối với hoạt động kinh doanh các sản phẩm, dịch vụ về dữ liệu theo quy định của Nghị định này.

3. Chủ trì, phối hợp với các cơ quan có liên quan triển khai xây dựng Trung tâm dữ liệu quốc gia đáp ứng các quy định, tiêu chuẩn, quy chuẩn kỹ thuật đối với trung tâm dữ liệu.

4. Chủ trì xây dựng, ban hành hoặc trình cơ quan nhà nước có thẩm quyền ban hành và hướng dẫn thi hành văn bản quy phạm pháp luật hướng dẫn thực hiện các quy định pháp luật về dữ liệu.

5. Chủ trì phối hợp Bộ Tư pháp, Văn phòng Chính phủ, Bộ Khoa học và Công nghệ và các cơ quan liên quan rà soát, tổng hợp đề xuất Chính phủ chỉ đạo các bộ, cơ quan, địa phương xây dựng, sửa đổi, bổ sung các văn bản liên quan đến việc triển khai, quản trị vận hành của Trung tâm dữ liệu quốc gia.

6. Tổ chức thực hiện kết nối, chia sẻ, điều phối dữ liệu giữa hệ thống thông tin, cơ sở dữ liệu của cơ quan, tổ chức, cá nhân với Cơ sở dữ liệu tổng hợp quốc gia thông qua Nền tảng chia sẻ, điều phối dữ liệu của Trung tâm dữ liệu quốc gia.

7. Bảo đảm hạ tầng công nghệ thông tin cho cơ quan Đảng, Nhà nước, tổ chức chính trị - xã hội phục vụ việc quản lý, quản trị, xử lý dữ liệu thuộc phạm vi quản lý tại Trung tâm dữ liệu quốc gia.

8. Chủ trì, phối hợp với Bộ Khoa học và Công nghệ thẩm định, đánh giá, kiểm tra, hỗ trợ giám sát và điều phối ứng phó sự cố an ninh mạng, an toàn thông tin trong quá trình xây dựng, triển khai, vận hành các hệ thống thông tin, cơ sở dữ liệu tại Trung tâm dữ liệu quốc gia.

9. Chủ trì, phối hợp với Bộ Khoa học và Công nghệ xây dựng tiêu chuẩn, quy chuẩn kỹ thuật hoặc hướng dẫn kỹ thuật về tổ chức, kết nối, chia sẻ, đồng bộ dữ liệu với Trung tâm dữ liệu quốc gia.

10. Xây dựng tiêu chuẩn kiến trúc hệ thống phần mềm tại Trung tâm dữ liệu quốc gia.

11. Hướng dẫn tổ chức phân loại dữ liệu của cơ quan Đảng, Nhà nước, tổ chức chính trị - xã hội; tổ chức, chỉ đạo công tác đào tạo, bồi dưỡng về chuyên môn, nghiệp vụ về dữ liệu trên phạm vi cả nước.

12. Xây dựng và vận hành Cổng dữ liệu quốc gia.

13. Bộ trưởng Bộ Công an quyết định mức chi cho hoạt động hỗ trợ kinh phí bảo đảm kết nối, chia sẻ; hỗ trợ bù đắp chi phí tạo lập, thu thập dữ liệu trên cơ sở thống nhất với Bộ trưởng Bộ Tài chính, Bộ trưởng Bộ Khoa học và Công nghệ.

Điều 27. Trách nhiệm của Bộ Quốc phòng

1. Chịu trách nhiệm trước Chính phủ trong thực hiện công tác quản lý nhà nước đối với các dữ liệu thuộc phạm vi quản lý.

2. Phối hợp với Bộ Công an, các cơ quan, tổ chức bố trí lực lượng, phương tiện thích hợp để phát hiện, ngăn chặn từ xa mọi hành vi xâm phạm Trung tâm

dữ liệu quốc gia cả về địa lý và trên không gian mạng.

3. Chủ trì quản lý hoạt động lưu trữ, bảo vệ dữ liệu, bảo đảm an ninh dữ liệu; quản lý, theo dõi, giám sát, tổ chức thực hiện kết nối, chia sẻ, điều phối dữ liệu giữa hệ thống thông tin, cơ sở dữ liệu; ứng dụng khoa học trong xử lý, quản lý, khai thác, sử dụng dữ liệu; quản lý, cấp phép chuyển dữ liệu ra nước ngoài; sử dụng quỹ phát triển dữ liệu quốc gia đối với các dữ liệu thuộc phạm vi quản lý của Bộ Quốc phòng.

Điều 28. Trách nhiệm của Bộ Khoa học và Công nghệ

1. Hướng dẫn cơ quan Đảng, Nhà nước, tổ chức chính trị - xã hội phát triển, hoàn thiện hạ tầng kỹ thuật công nghệ thông tin và việc xây dựng tiêu chuẩn, quy chuẩn kỹ thuật về tổ chức, kết nối, chia sẻ, đồng bộ dữ liệu; thực hiện chuẩn hoá, kết nối, chia sẻ dữ liệu, tính toán tối ưu giữa việc đầu tư hạ tầng mới và sử dụng hạ tầng do Trung tâm dữ liệu quốc gia cung cấp.

2. Rà soát, đánh giá năng lực mạng truyền số liệu chuyên dùng của các cơ quan để xây dựng phương án nâng cấp, bảo đảm các đơn vị có thể truy cập, quản trị hệ thống đặt tại Trung tâm dữ liệu quốc gia thông qua mạng truyền số liệu chuyên dùng.

3. Phối hợp với Bộ Công an và cơ quan có liên quan trong nghiên cứu làm chủ và ứng dụng các công nghệ số, dữ liệu số hình thành các sản phẩm, dịch vụ phục vụ phát triển chính phủ số, chính quyền số và phát triển kinh tế - xã hội thông qua các Chương trình khoa học và công nghệ trọng điểm cấp quốc gia.

4. Phối hợp với Bộ Công an trong việc xác định mức chi cho hoạt động hỗ trợ kinh phí bảo đảm kết nối, chia sẻ; hỗ trợ bù đắp chi phí tạo lập, thu thập dữ liệu.

Điều 29. Trách nhiệm của Văn phòng Chính phủ

1. Chủ trì xây dựng yêu cầu chức năng, nghiệp vụ, giao diện; hỗ trợ, hướng dẫn các bộ, ngành, địa phương xử lý các vấn đề về chức năng, quy trình nghiệp vụ, dữ liệu của Cổng Dịch vụ công quốc gia; phối hợp với Bộ Công an quản trị, vận hành Cổng Dịch vụ công quốc gia tại Trung tâm dữ liệu quốc gia; thực hiện các nhiệm vụ khác về phát triển Cổng Dịch vụ công quốc gia theo yêu cầu của Chính phủ, Thủ tướng Chính phủ; quản lý, vận hành Cơ sở dữ liệu quốc gia về thủ tục hành chính;

2. Phối hợp Bộ Công an và các đơn vị liên quan đánh giá nhu cầu, thực hiện chuyển dịch hạ tầng kỹ thuật công nghệ thông tin các hệ thống thông tin phục vụ chỉ đạo, điều hành của Chính phủ, Thủ tướng Chính phủ để đặt tại Trung tâm dữ liệu quốc gia.

Điều 30. Trách nhiệm của Ban Cơ yếu Chính phủ

1. Chủ trì phối hợp với các đơn vị có liên quan triển khai các sản phẩm

mã hóa, giải mã dữ liệu.

2. Ban Cơ yếu Chính phủ giúp Bộ trưởng Bộ Quốc phòng thực hiện nhiệm vụ quản lý nhà nước đối với dữ liệu về cơ yếu.

3. Phối hợp với Bộ Công an triển khai các giải pháp bảo đảm an toàn, xác thực và bảo mật thông tin dùng mật mã; triển khai dịch vụ chứng thực chữ ký số chuyên dùng Chính phủ cho các hệ thống thông tin và cơ sở dữ liệu của cơ quan Đảng, Nhà nước, tổ chức chính trị - xã hội.

Điều 31. Trách nhiệm của Bộ Tài chính

1. Phối hợp với Bộ Công an trong việc xác định mức chi cho hoạt động hỗ trợ kinh phí bảo đảm kết nối, chia sẻ; hỗ trợ bù đắp chi phí tạo lập, thu thập dữ liệu.

2. Ban hành Thông tư quy định thu phí khai thác và sử dụng thông tin trong cơ sở dữ liệu tổng hợp quốc gia, cơ sở dữ liệu quốc gia, cơ sở dữ liệu chuyên ngành trên cơ sở đề xuất của các bộ, cơ quan ngang bộ.

Điều 32. Trách nhiệm của các bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ và Ủy ban nhân dân tỉnh, thành phố trực thuộc trung ương

1. Chủ trì, phối hợp với Bộ Công an, Bộ Quốc phòng và cơ quan có liên quan quản lý hoạt động thu thập, cập nhật, điều chỉnh, sao chép, chia sẻ, chuyển giao, xóa, hủy dữ liệu, lưu trữ, bảo vệ dữ liệu thuộc phạm vi quản lý.

2. Thực hiện đồng bộ dữ liệu thuộc phạm vi quản lý về Trung tâm dữ liệu quốc gia theo quy định của Nghị định này và phối hợp với Bộ Công an thực hiện giám sát và đối soát để bảo đảm tính chính xác của dữ liệu.

3. Các bộ, ngành, địa phương phối hợp Văn phòng Chính phủ, Bộ Công an và các đơn vị có liên quan thực hiện tái cấu trúc quy trình, sửa đổi các văn bản pháp lý theo lộ trình thu thập, cập nhật, đồng bộ dữ liệu về Cơ sở dữ liệu tổng hợp quốc gia.

4. Thực hiện nâng cấp, bảo trì, sửa chữa hạ tầng, thiết bị của cơ quan khi sử dụng hạ tầng của Trung tâm dữ liệu quốc gia.

5. Kiến nghị Bộ Tài chính về mức thu, nộp, miễn, giảm, quản lý và sử dụng đối với phí khai thác và sử dụng thông tin trong cơ sở dữ liệu tổng hợp quốc gia, cơ sở dữ liệu quốc gia, cơ sở dữ liệu chuyên ngành thuộc ngành, lĩnh vực quản lý.

Chương VI ĐIỀU KHOẢN THI HÀNH

Điều 33. Hiệu lực thi hành

Nghị định này có hiệu lực thi hành từ ngày 01 tháng 7 năm 2025.

Điều 34. Trách nhiệm thi hành

Bộ trưởng các bộ, Thủ trưởng các cơ quan ngang bộ, cơ quan thuộc Chính phủ, Chủ tịch Ủy ban nhân dân các tỉnh, thành phố trực thuộc trung ương và các cơ quan, tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành Nghị định này.

Nơi nhận:

- Ban Bí thư Trung ương Đảng;
- Thủ tướng, các Phó Thủ tướng Chính phủ;
- Các bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ;
- HĐND, UBND các tỉnh, thành phố trực thuộc trung ương;
- Văn phòng Trung ương và các Ban của Đảng;
- Văn phòng Tổng Bí thư;
- Văn phòng Chủ tịch nước;
- Hội đồng Dân tộc và các Ủy ban của Quốc hội;
- Văn phòng Quốc hội;
- Tòa án nhân dân tối cao;
- Viện kiểm sát nhân dân tối cao;
- Kiểm toán nhà nước;
- Ủy ban Trung ương Mặt trận Tổ quốc Việt Nam;
- Cơ quan trung ương của các đoàn thể;
- VPCP: BTCN, các PCN, Trợ lý TTg, TGĐ Cổng TTĐT, các Vụ, Cục, đơn vị trực thuộc, Công báo;
- Lưu: VT, KSTT (2) ~~70~~

TM. CHÍNH PHỦ
KT. THỦ TƯỚNG
PHÓ THỦ TƯỚNG



Nguyễn Chí Dũng