|  |  |
| --- | --- |
| **CHÍNH PHỦ**  Số: /2025/NĐ-CP | **CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM**  **Độc lập - Tự do - Hạnh phúc**  *Hà Nội, ngày tháng năm 2025* |

|  |
| --- |
| **DỰ THẢO 02** |

**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 19 tháng 6 năm 2015;*

*Căn cứ Luật sửa đổi, bổ sung một số điều của Luật Tổ chức Chính phủ và Luật Tổ chức chính quyền địa phương ngày 22 tháng 11 năm 2019;*

*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.*

**QUY ĐỊNH CHUNG**

# 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.

# Đối tượng áp dụng

1. Cơ quan, tổ chức, cá nhân Việt Nam.

2. Cơ quan, tổ chức, cá nhân nước ngoài tại Việt Nam.

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

**CÁC HOẠT ĐỘNG XỬ LÝ DỮ LIỆU**

# Tiêu chí xác định dữ liệu quan trọng

Việc xác định dữ liệu quan trọng phải dựa trên mức độ tác động của dữ liệu đến lĩnh vực, nhóm, khu vực cụ thể, có thể tác động quốc phòng, an ninh, đối ngoại, kinh tế vĩ mô, ổn định xã hội, sức khỏe và an toàn cộng đồng (không bao gồm bí mật nhà nước), bao gồm:

1. Ảnh hưởng đến an ninh quốc gia, độc lập, chủ quyền, thống nhất và toàn vẹn lãnh thổ của Tổ quốc; bảo vệ Đảng, Nhà nước, Nhân dân và chế độ xã hội chủ nghĩa; 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, khoa học và công nghệ; bảo vệ các lợi ích khác của quốc gia; bảo vệ khối đại đoàn kết toàn dân tộc.

2. Ảnh hưởng đến kế hoạch phát triển quan hệ với nước ngoài, tổ chức quốc tế hoặc chủ thể khác của pháp luật quốc tế, lợi ích quốc gia và an ninh hợp tác quốc tế và các lĩnh vực khác, dự án lớn ở nước ngoài và các tổ chức nhân sự, sự an toàn của các nguồn năng lượng ở nước ngoài và sự an toàn của các tuyến hàng hải chiến lược.

3. Ảnh hưởng đến phát triển kinh tế, kinh tế vĩ mô, huyết mạch kinh tế quốc gia, cơ sở hạ tầng của ngành kinh tế quan trọng.

4. Ảnh hưởng đến tính mạng, sức khỏe, danh dự, nhân phẩm, tài sản, quyền, lợi ích hợp pháp của cơ quan, tổ chức, cá nhân.

# Tiêu chí xác định dữ liệu cốt lõi

Việc xác định dữ liệu cốt lõi phải dựa trên mức độ tác động của dữ liệu đến các lĩnh vực, các nhóm, các khu vực cụ thể, tác động trực tiếp quốc phòng, an ninh, đối ngoại, kinh tế vĩ mô, ổn định xã hội, sức khỏe và an toàn cộng đồng (không bao gồm bí mật nhà nước), bao gồm:

1. Chủ trương, chính sách của Đảng và Nhà nước về đối nội, đối ngoại; Hoạt động của Ban Chấp hành Trung ương, Bộ Chính trị, Ban Bí thư và lãnh đạo Đảng, Nhà nước; Chiến lược, đề án về dân tộc, tôn giáo và công tác dân tộc, tôn giáo liên quan đến bảo vệ an ninh quốc gia, bảo đảm trật tự, an toàn xã hội.

2. Chiến lược, kế hoạch, phương án, hoạt động bảo vệ Tổ quốc, phòng thủ đất nước, bảo vệ an ninh quốc gia, bảo đảm trật tự, an toàn xã hội; chương trình, dự án, đề án đặc biệt quan trọng.

3. Tổ chức và hoạt động của lực lượng vũ trang nhân dân, lực lượng cơ yếu.

4. Công trình, mục tiêu về quốc phòng, an ninh, cơ yếu; các loại vũ khí, khí tài, phương tiện quyết định khả năng phòng thủ đất nước, bảo vệ an ninh quốc gia, bảo đảm trật tự, an toàn xã hội; sản phẩm mật mã của cơ yếu.

5. Dữ liệu cơ sở và hạ tầng dữ liệu và truyền thông quốc gia để phục vụ quốc phòng, an ninh.

6. Chiến lược, kế hoạch, đề án phát triển báo chí, xuất bản, in, phát hành, bưu chính, viễn thông và Internet, tần số vô tuyến điện, công nghệ dữ liệu, công nghiệp công nghệ dữ liệu, an toàn dữ liệu mạng, điện tử, phát thanh và truyền hình, dữ liệu điện tử, thông tấn, dữ liệu đối ngoại, dữ liệu cơ sở và hạ tầng dữ liệu và truyền thông quốc gia để phục vụ quốc phòng, an ninh.

7. Thiết kế kỹ thuật, sơ đồ, số liệu về thiết bị của hệ thống dữ liệu quan trọng về an ninh quốc gia, hệ thống dữ liệu quan trọng quốc gia và hệ thống mạng dữ liệu dùng riêng phục vụ cơ quan, tổ chức của Đảng, Nhà nước.

8. Chiến lược, kế hoạch, đề án phát triển quan hệ với nước ngoài, tổ chức quốc tế hoặc chủ thể khác của pháp luật quốc tế; tình hình, phương án, kế hoạch, hoạt động đối ngoại của cơ quan Đảng, Nhà nước.

9. Dữ liệu, thỏa thuận được trao đổi, ký kết giữa Việt Nam với nước ngoài, tổ chức quốc tế hoặc chủ thể khác của pháp luật quốc tế.

10. Dữ liệu do nước ngoài, tổ chức quốc tế hoặc chủ thể khác của pháp luật quốc tế chuyển giao theo điều ước quốc tế mà nước Cộng hòa xã hội chủ nghĩa Việt Nam là thành viên và thỏa thuận quốc tế có liên quan.

11. Chiến lược, kế hoạch đầu tư và dự trữ quốc gia bảo đảm quốc phòng, an ninh; đấu thầu phục vụ bảo vệ an ninh quốc gia.

12. Dữ liệu về phương án, kế hoạch thu, đổi, phát hành tiền; thiết kế mẫu, chế tạo bản in, khuôn đúc, công nghệ in, đúc tiền và giấy tờ có giá; số lượng, nơi lưu giữ kim loại quý hiếm, đá quý và vật quý hiếm khác của Nhà nước.

13. Dữ liệu về quá trình xây dựng quy hoạch cấp quốc gia, quy hoạch vùng, quy hoạch tỉnh, quy hoạch đơn vị hành chính - kinh tế đặc biệt, quy hoạch đô thị, quy hoạch nông thôn; dữ liệu về quy hoạch hệ thống kho dự trữ quốc gia, quy hoạch hệ thống các công trình quốc phòng, khu quân sự, kho đạn dược, công nghiệp quốc phòng, an ninh.

14. Dữ liệu về tài nguyên và môi trường bao gồm tài nguyên nước, môi trường, địa chất, khoáng sản, khí tượng thủy văn, đất đai, biển, hải đảo, đo đạc và bản đồ.

15. Dữ liệu về khoa học và công nghệ gồm sáng chế, công nghệ mới phục vụ quốc phòng, an ninh hoặc có ý nghĩa đặc biệt quan trọng đối với phát triển kinh tế - xã hội; Dữ liệu về năng lượng nguyên tử, an toàn bức xạ và hạt nhân liên quan đến quốc phòng, an ninh; nhiệm vụ khoa học và công nghệ đặc biệt, nhiệm vụ khoa học và công nghệ cấp quốc gia liên quan đến quốc phòng, an ninh.

16. Chủng, giống vi sinh vật mới phát hiện liên quan đến sức khỏe, tính mạng con người; mẫu vật, nguồn gen, vùng nuôi trồng dược liệu quý hiếm.

17. Quy trình sản xuất dược liệu, thuốc sinh học quý hiếm.

18. Dữ liệu, tài liệu, số liệu điều tra về dân số.

19. Dữ liệu về thanh tra, kiểm tra, giám sát, xử lý vi phạm, giải quyết khiếu nại, tố cáo và phòng, chống tham nhũng.

# Hoạt động lưu trữ dữ liệu

1. Trung tâm dữ liệu quốc gia cung cấp các dịch vụ lưu trữ dữ liệu bao gồm:

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 quốc gia, cho phép chủ quản cơ sở dữ liệu quốc gia, 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 quốc gia, 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 quốc gia, cơ sở dữ liệu và hệ thống thông tin khác.

2. Tổ chức, cá nhân không phải là cơ quan nhà nước sử dụng dịch vụ quy định tại điểm b, điểm c khoản 1 Điều này để lưu trữ dữ liệu trên cơ sở hạ tầng của Trung tâm dữ liệu quốc gia.

# Truy cập, truy xuất dữ liệu

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

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 cập khác theo quy trình do chủ quản cơ sở dữ liệu quy định.

2. Cơ quan nhà nước phải ban hành quy trình kỹ thuật về truy cập, truy xuất dữ liệu đối với cơ sở dữ liệu do mình quản lý, gồm các nội dung:

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) Các nội dung khác do chủ quản cơ sở dữ liệu quy định.

3. Các công cụ để truy cập, truy xuất dữ liệu do cơ quan nhà nước cung cấp gồm:

a) Cổng dịch vụ công quốc gia;

b) Hệ thống, phần mềm quản lý, khai thác, cung cấp dịch vụ dữ liệu, cổng dữ liệu mở, cổng dịch vụ dữ liệu của Trung tâm dữ liệu quốc gia;

c) Các hệ thống thông tin, phần mềm được cung cấp bởi chủ quản cơ sở dữ liệu.

4. Việc truy cập, truy xuất dữ liệu phải bảo đảm tuân thủ những nguyên tắc sau:

a) Bảo đảm hợp pháp, công bằng và minh bạch khi truy cập, truy xuất dữ liệu;

b) Chỉ truy cập dữ liệu trong phạm vi thẩm quyền và cần thiết cho mục đích được xác định ban đầu, không truy cập nhằm mục đích khác;

c) Việc truy cập các dữ liệu quan trọng, dữ liệu cốt lõi phải được quản lý chặt chẽ bằng quy chế và biện pháp kỹ thuật xác thực người truy cập, nội dung truy cập để bảo đảm không xâm phạm lợi ích của quốc gia, cơ quan, tổ chức, cá nhân; ghi nhận, lưu trữ lịch sử quá trình truy cập;

d) Bảo bảo đảm mật và sử dụng các biện pháp bảo mật phù hợp khi truy cập, truy xuất;

đ) Tuân thủ quy định, quy trình truy cập, truy xuất dữ liệu;

e) Cơ quan, tổ chức, cá nhân có liên quan sử dụng công cụ truy xuất dữ liệu có trách nhiệm sử dụng các biện pháp kỹ thuật để bảo vệ dữ liệu vào quy trình thiết kế ngay từ đầu nhằm bảo vệ dữ liệu;

g) Dữ liệu truy xuất phải được sự đồng ý của chủ quản dữ liệu và được sử dụng đúng mục đích trừ trường hợp luật có quy định khác.

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

1. Cơ quan nhà nước sẵn sàng về mặt tổ chức, kỹ thuật để tạo điều kiện cho tổ chức, cá nhân cung cấp dữ liệu tự nguyện nhằm mang lại niềm tin rằng dữ liệu được tổ chức, cá nhân cung cấp đang phục vụ mục tiêu vì lợi ích chung gồm:

a) Không sử dụng dữ liệu cho các mục tiêu khác ngoài mục tiêu vì lợi ích chung mà chủ thể dữ liệu, chủ sở hữu dữ liệu xác định;

b) Cung cấp công cụ cho phép chủ thể dữ liệu, chủ sở hữu dữ liệu rút lại hoặc sửa đổi sự đồng ý, cập nhật thông tin về việc sử dụng dữ liệu họ cung cấp;

c) Thực hiện các biện pháp để bảo đảm mức độ bảo mật phù hợp cho việc lưu trữ và xử lý dữ liệu, bảo vệ quyền và lợi ích của chủ thể dữ liệu, chủ sở hữu dữ liệu liên quan đến dữ liệu của họ;

d) Thông báo cho chủ thể dữ liệu, chủ sở hữu dữ liệu trong trường hợp có bất kỳ hành vi chuyển giao, truy cập hoặc sử dụng trái phép nào đối với dữ liệu mà tổ chức, cá nhân đã cung cấp.

2. Các hình thức hỗ trợ thực hiện kết nối, chia sẻ dữ liệu:

a) Hỗ trợ về kỹ thuật, bao gồm: 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 về tài chính, bao gồm: Hỗ trợ kinh phí 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 về nhân lực, bao gồm: 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 do người đứng đầu cơ quan quản lý cơ sở dữ liệu quyết định.

3. Người đứng đầu cơ quan quản lý cơ sở dữ liệu, hệ thống thông tin quyết định việc tiếp nhận dữ liệu được chia sẻ từ các tổ chức, cá nhân là chủ sở hữu dữ liệu.

4. 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 thực hiện kết nối, chia sẻ dữ liệu cho cơ quan nhà nước thuộc phạm vi quản lý.

# 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, chống 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 vì lợi ích chung.

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. Tổ chức, cá nhân phải thực hiện cung cấp dữ liệu cho cơ quan Đảng, Nhà nước, tổ chức chính trị - xã hội trong trường hợp đặc biệt khi được yêu cầu của cơ quan có thẩm quyền được thực hiện như sau:

a) Yêu cầu cung cấp dữ liệu phải được thể hiện bằng văn bản. Trường hợp đặc biệt không thể ra yêu cầu bằng văn bản thì người có thẩm quyền quyết định được quyết định yêu cầu dữ liệu bằng lời nói để thực hiện nhiệm vụ được giao nhưng phải có giấy xác nhận;

b) Yêu cầu cung cấp dữ liệu phải được giao cho cá nhân, tổ chức là chủ sở hữu dữ liệu, người đại diện hợp pháp hoặc người đang quản lý, sử dụng hợp pháp dữ liệu.

3. Khi yêu cầu tổ chức, cá nhân cung cấp dữ liệu trong trường hợp đặc biệt, cơ quan Đảng, Nhà nước, tổ chức chính trị - xã hội có trách nhiệm:

a) Chỉ rõ dữ liệu được yêu cầu;

b) Giải thích mục đích sử dụng dữ liệu và thời hạn sử dụng;

c) Nêu cơ sở pháp lý cho việc yêu cầu dữ liệu;

d) Chỉ định thời hạn cần cung cấp dữ liệu. Trước thời hạn đó chủ quản dữ liệu, chủ sở hữu dữ liệu có thể yêu cầu cơ quan Đảng, Nhà nước, tổ chức chính trị - xã hội sửa đổi hoặc rút lại yêu cầu;

đ) Thông báo cho chủ quản dữ liệu, chủ sở hữu dữ liệu về các chế tài sẽ được áp dụng trong trường hợp không thực hiện yêu cầu.

4. Yêu cầu cung cấp dữ liệu phải bảo đảm:

a) Được thể hiện bằng ngôn ngữ rõ ràng, ngắn gọn và dễ hiểu đối với chủ quản dữ liệu, chủ sở hữu dữ liệu;

b) Xác định rõ về 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;

c) Tôn trọng các mục đích hợp pháp của chủ quản dữ liệu, chủ sở hữu dữ liệu, bảo vệ bí mật kinh doanh, bí mật cá nhân.

5. Thẩm quyền yêu cầu cung cấp dữ liệu

Bộ trưởng, Thủ trưởng cơ quan ngang Bộ, Chủ tịch Ủy ban nhân dân cấp tỉnh, thành phố có thẩm quyền yêu cầu cung cấp dữ liệu trong phạm vi nhiệm vụ, quyền hạn của mình.

6. 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.

7. 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.

8. 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.

# Xác nhận, xác thực dữ liệu

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

a) Chủ quản dữ liệu xác nhận 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 do mình chủ quản;

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, chủ thể dữ liệu hoặc tổ chức cung cấp dịch vụ xác thực điện tử nhưng không được trái quy định pháp luật;

d) Chủ sở hữu dữ liệu, chủ quản dữ liệu chịu trách nhiệm về chất lượng dữ liệu được xác nhận;

đ) Chủ sở hữu dữ liệu, chủ thể dữ liệu chịu trách nhiệm về mức độ tin cậy, hợp pháp của dữ liệu do mình cung cấp và xác nhận.

2. Dữ liệu được xác thực bởi chủ quản dữ liệu, chủ sở hữu dữ liệu hoặc tổ chức cung cấp dịch vụ xác thực điện tử. Dữ liệu được xác thực có giá trị tương đương với dữ liệu gốc được lưu trữ tại cơ sở dữ liệu quốc gia, cơ sở dữ liệu chuyên ngành, cơ sở dữ liệu khác.

3. Xác thực dữ liệu bao gồm:

a) Xác thực dữ liệu gắn với danh tính điện tử;

b) Xác thực dữ liệu không gắn với danh tính điện tử.

4. Chủ quản dữ liệu, tổ chức cung cấp dịch vụ xác thực điện tử có trách nhiệm xây dựng quy trình xác nhận, xác thực dữ liệu trong phạm vi dữ liệu mình quản lý hoặc dịch vụ dữ liệu do mình cung cấp.

5. Việc xác nhận, xác thực dữ liệu phải được thực hiện chính xác và hợp pháp đối với nội dung do chủ thể yêu cầu xác nhận, xác thực.

6. Phạm vi và thời gian có giá trị của việc xác thực dữ liệu do tổ chức cung cấp dịch vụ xác thực điện tử, chủ sở hữu dữ liệu, chủ quản dữ liệu quyết định.

# Công khai dữ liệu

1. Các dữ liệu không được phép công khai gồm:

a) Dữ liệu cá nhân mà không được chủ thể dữ liệu đồng ý;

b) Dữ liệu là bí mật nhà nước; dữ liệu tác động đến quốc phòng, an ninh;

c) Dữ liệu nếu công khai sẽ gây nguy hại đến lợi ích của Đảng, Nhà nước, lợi ích quốc gia, quan hệ đối ngoại; đạo đức xã hội, sức khỏe của cộng đồng; gây nguy hại đến tính mạng, sức khỏe, quyền và lợi ích hợp pháp của tổ chức, cá nhân.

2. Dữ liệu được công khai có điều kiện gồm:

a) Dữ liệu liên quan đến bí mật kinh doanh được công khai trong trường hợp chủ sở hữu bí mật kinh doanh đó đồng ý theo quy định pháp luật;

b) Dữ liệu liên quan đến bí mật đời sống riêng tư, bí mật cá nhân được công khai trong trường hợp được người đó đồng ý; dữ liệu liên quan đến bí mật gia đình được công khai trong trường hợp được các thành viên gia đình đồng ý;

c) Trong quá trình thực hiện chức năng, nhiệm vụ, quyền hạn của mình, người đứng đầu cơ quan nhà nước, tổ chức chính trị - xã hội quyết định việc công khai dữ liệu mà không cần có sự đồng ý theo quy định tại điểm a và điểm b Khoản này trong trường hợp vì lợi ích công cộng, sức khỏe của cộng đồng và các trường hợp khác theo quy định của pháp luật.

3. 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 cơ sở dữ liệu thực hiện công khai dữ liệu mở dưới hình thức:

a) Cổng dữ liệu mở của Trung tâm dữ liệu quốc gia;

b) Các cổng dữ liệu mở của bộ, ngành, địa phương và các hệ thống, nền tảng khác.

4. Bộ Công an tổng hợp, công bố, công khai danh mục dữ liệu mở do cơ quan nhà nước quản lý.

# 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 định 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, Giám đốc Công an tỉnh, thành phố trực thuộc trung ương trong phạm vi quản lý quyết định việc áp dụng các biện pháp để giải mã 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, Chỉ huy trưởng Bộ Chỉ huy quân sự tỉnh, thành phố trực thuộc Trung ương trong phạm vi quản lý quyết định việc áp dụng các biện pháp để giải mã dữ liệu mà không cần chủ sở hữu dữ liệu, chủ quản dữ liệu đồng ý, trừ trường hợp quy định tại khoản 2 Điều này.

# Chuyển, xử lý dữ liệu xuyên biên giới

1. Hoạt động cung cấp, chuyển dữ liệu ra nước ngoài, cho tổ chức, cá nhân nước ngoài phải bảo bảo đảm vệ quyền và lợi ích hợp pháp của chủ thể dữ liệu, bảo vệ an ninh, quốc phòng và lợi ích quốc gia, lợi ích công cộng.

2. Chủ quản dữ liệu khi cần chuyển, xử lý dữ liệu cốt lõi, dữ liệu quan trọng xuyên biên giới thì thực hiện tự đánh giá rủi ro theo yêu cầu tại khoản 3 Điều này, lập Hồ sơ đánh giá tác động chuyển, xử lý dữ liệu xuyên biên giới và thực hiện các thủ tục theo quy định tại khoản 4 Điều này. Đối với dữ liệu cá nhân thì thực hiện theo quy định của pháp luật về bảo vệ dữ liệu cá nhân, trừ trường hợp dữ liệu cá nhân thuộc danh mục dữ liệu cốt lõi, dữ liệu quan trọng thì thực hiện theo quy định tại Nghị định này.

3. Bên chuyển dữ liệu phải tự đánh giá rủi ro chuyển, xử lý dữ liệu, tập trung vào 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 ở nước ngoài;

b) Quy mô, phạm vi, loại và độ nhạy cảm của dữ liệu được chuyển ra nước ngoài, xử lý ở nước ngoài và những rủi ro mà việc này có thể gây ra cho an ninh quốc gia, hoạt động kinh tế, ổn định xã hội, lợi ích công cộng hoặc quyền và lợi ích hợp pháp của cá nhân hoặc tổ chức;

c) Trách nhiệm và nghĩa vụ mà bên nhận ở nước ngoài đã cam kết đảm nhận, cũng như các biện pháp quản lý và kỹ thuật và khả năng thực hiện trách nhiệm và nghĩa vụ có thể bảo đảm an toàn cho dữ liệu hay không;

d) Rủi ro dữ liệu sẽ bị giả mạo, phá hủy, rò rỉ, mất, chuyển giao hoặc có được hoặc sử dụng bất hợp pháp trong hoặc sau khi dữ liệu được chuyển ra nước ngoài, xử lý ở nước ngoài;

đ) Hợp đồng hoặc văn bản có hiệu lực pháp luật khác (sau đây gọi chung là văn bản pháp lý) được soạn thảo với bên nhận ở nước ngoài có thỏa thuận đầy đủ về trách nhiệm và nghĩa vụ bảo vệ an toàn dữ liệu hay không;

e) Các vấn đề khác có thể ảnh hưởng đến an toàn dữ liệu.

4. Bên chuyển dữ liệu phải thỏa thuận rõ trách nhiệm và nghĩa vụ bảo vệ an toàn dữ liệu trong các Hợp đồng hoặc các văn bản có hiệu lực pháp lý khác được ký kết với bên nhận ở nước ngoài, bao gồm tối thiểu các nội dung sau:

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

b) Địa điểm và thời gian lưu trữ dữ liệu ở nước ngoài, cũng như các biện pháp xử lý dữ liệu được trích suất sau khi đạt đến thời gian lưu giữ, mục đích đã thỏa thuận được hoàn thành hoặc tài liệu pháp lý bị chấm dứt;

c) Yêu cầu ràng buộc đối với người nhận ở nước ngoài để chuyển lại dữ liệu đã xuất cho tổ chức hoặc cá nhân khác;

d) Các biện pháp bảo mật mà bên nhận ở nước ngoài sẽ sử dụng khi có sự thay đổi đáng kể trong kiểm soát thực tế hoặc phạm vi hoạt động của mình hoặc khi có sự thay đổi trong các chính sách và quy định bảo vệ an ninh dữ liệu của quốc gia hoặc khu vực nơi họ đặt trụ sở hoặc khi xảy ra các trường hợp bất khả kháng khác, gây khó khăn cho việc bảo đảm an ninh dữ liệu;

đ) Biện pháp khắc phục hậu quả, trách nhiệm do vi phạm hợp đồng, biện pháp giải quyết tranh chấp đối với hành vi vi phạm nghĩa vụ bảo vệ an toàn dữ liệu đã thỏa thuận tại các văn bản quy phạm pháp luật;

e) Khi có nguy cơ thay đổi, phá hủy, rò rỉ, mất mát, chuyển giao hoặc thu thập bất hợp pháp hoặc sử dụng bất hợp pháp dữ liệu đã xuất cần thực hiện đúng các yêu cầu ứng phó khẩn cấp và cách thức và phương tiện để bảo đảm rằng tổ chức, cá nhân là chủ thể dữ liệu được bảo vệ quyền và lợi ích hợp pháp của họ.

5. Hồ sơ đánh giá tác động chuyển, xử lý dữ liệu xuyên biên giới, gồm:

a) Thông tin và chi tiết liên lạc của Bên chuyển dữ liệu và Bên tiếp nhận dữ liệu;

b) Họ tên, chi tiết liên lạc của tổ chức, cá nhân phụ trách của Bên chuyển dữ liệu có liên quan tới việc chuyển và tiếp nhận dữ liệu;

c) Mô tả và luận giải mục tiêu của các hoạt động xử lý dữ liệu sau khi được chuyển ra nước ngoài, xử lý dữ liệu ở nước ngoài;

d) Mô tả và làm rõ loại dữ liệu chuyển ra nước ngoài, xử lý ở nước ngoài;

đ) Mô tả và nêu rõ sự tuân thủ quy định bảo vệ dữ liệu, chi tiết các biện pháp bảo vệ dữ liệu được áp dụng;

e) Đánh giá mức độ ảnh hưởng của việc xử lý dữ liệu; hậu quả, thiệt hại không mong muốn có khả năng xảy ra, các biện pháp giảm thiểu hoặc loại bỏ nguy cơ, tác hại đó;

g) Sự đồng ý của chủ thể dữ liệu theo quy định trên cơ sở biết rõ cơ chế phản hồi, khiếu nại khi có sự cố hoặc yêu cầu phát sinh;

h) Hợp đồng hoặc các văn bản có hiệu lực pháp lý khác được soạn thảo với bên nhận dữ liệu có thỏa thuận đầy đủ về trách nhiệm và nghĩa vụ bảo vệ an toàn dữ liệu, đảm bảo hoạt động xử lý dữ liệu của bên nhận dữ liệu tuân thủ các tiêu chuẩn về an ninh, an toàn tương đương với các tiêu chuẩn được quy định về bảo vệ dữ liệu cốt lõi, dữ liệu quan trọng tại Việt Nam.

Bên chuyển dữ liệu ra nước ngoài, xử lý dữ liệu ở nước ngoài chịu trách nhiệm pháp lý về tính xác thực của các hồ sơ đánh giá tác động.

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

a) Chủ quản dữ liệu lập và gửi Hồ sơ đánh giá tác động chuyển, xử lý dữ liệu xuyên biên giới đến Bộ Công an, trừ trường hợp thuộc lĩnh vực quân sự, quốc phòng, cơ yếu thì gửi đến 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 và yêu cầu bên chuyển dữ liệu ra nước ngoài, chuyển dữ liệu cho tổ chức, cá nhân nước ngoài bổ sung, hoàn thiện Hồ sơ đánh giá tác động chuyển dữ liệu ra nước ngoài trong trường hợp hồ sơ chưa đầy đủ và đúng quy định.

Trong quá trình đánh giá tác động, nếu phát hiện hồ sơ, tài liệu bên chuyển dữ liệu không đáp ứng các yêu cầu, đơn vị chịu trách nhiệm thuộc Bộ Quốc phòng, Bộ Công an có thể yêu cầu bên chuyển dữ liệu bổ sung hoặc điều chỉnh. Trong trường hợp bên chuyển dữ liệu không bổ sung hoặc điều chỉnh mà không có lý do chính đáng, đơn vị chịu trách nhiệm thuộc Bộ Quốc phòng, Bộ Công an có thể chấm dứt đánh giá tác động.

c) Đơn vị chịu trách nhiệm thuộc Bộ Quốc phòng, Bộ Công an hoàn thành đánh giá tác động trong thời hạn 10 ngày làm việc kể từ ngày nhận được hồ sơ đầy đủ, hợp lệ. Khi cần bổ sung hoặc điều chỉnh hồ sơ, tài liệu, thời gian có thể được kéo dài nhưng không vượt quá 5 ngày.

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 ở nước ngoài.

7. Trường hợp dữ liệu cần chuyển ra nước ngoài, xử lý ở nước ngoài là dữ liệu quan trọng:

a) Tối thiểu 5 ngày trước khi thực hiện chuyển ra nước ngoài, xử lý ở nước ngoài, chủ quản dữ liệu lập và gửi hồ sơ đánh giá tác động chuyển, xử lý dữ liệu xuyên biên giới kèm thông báo về việc chuyển, xử lý dữ liệu quan trọng xuyên biên giới đến các Bộ Quốc phòng nếu là dữ liệu thuộc lĩnh vực đến các Bộ Quốc phòng nếu là dữ liệu thuộc lĩnh vực quân sự, quốc phòng, cơ yếu; gửi đến Bộ Công an nếu là dữ liệu trong các lĩnh vực khác;

b) Sau 5 ngày, nếu không nhận được phản hồi của đơn vị chịu trách nhiệm thuộc Bộ Quốc phòng, Bộ Công an về việc đánh giá không đạt, chủ quản dữ liệu quyết định việc chuyển dữ liệu quan trọng ra nước ngoài, xử lý dữ liệu ở nước ngoài;

c) 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 và yêu cầu bên chuyển dữ liệu ra nước ngoài, chuyển dữ liệu cho tổ chức, cá nhân nước ngoài bổ sung, hoàn thiện Hồ sơ đánh giá tác động chuyển dữ liệu ra nước ngoài trong trường hợp hồ sơ chưa đầy đủ và đúng quy định;

d) Trong quá trình đánh giá tác động, nếu phát hiện ra rằng hồ sơ, tài liệu bên chuyển dữ liệu không đáp ứng các yêu cầu, đơn vị chịu trách nhiệm thuộc Bộ Quốc phòng, Bộ Công an có thể yêu cầu bên chuyển dữ liệu bổ sung hoặc điều chỉnh. Trong trường hợp bên chuyển dữ liệu không bổ sung hoặc điều chỉnh mà không có lý do chính đáng, đơn vị chịu trách nhiệm thuộc Bộ Quốc phòng, Bộ Công an có thể chấm dứt đánh giá tác động và yêu cầu Bên chuyển dữ liệu ra nước ngoài ngừng chuyển ra nước ngoài, ngừng xử lý ở nước ngoài dữ liệu quan trọng.

8. Việc đánh giá tác động của cơ quan có thẩm quyền tập trung vào việc đánh giá các rủi ro mà hoạt động chuyển dữ liệu ra nước ngoài, xử lý dữ liệu ở nước ngoài 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, và 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 nơi người nhận ở nước ngoài cư trú đối với tính bảo mật của dữ liệu xuất khẩu; Mức độ bảo vệ dữ liệu của người nhận ở nước ngoài có đáp ứng các yêu cầu của luật, quy định hành chính và tiêu chuẩn quốc gia bắt buộc của Việt Nam hay không;

c) Quy mô, phạm vi, loại và độ nhạy của dữ liệu xuất khẩu, và nguy cơ bị giả mạo, phá hủy, rò rỉ, mất, chuyển giao hoặc thu được hoặc sử dụng bất hợp pháp trong hoặc sau khi rời khỏi đất nước;

d) Liệu bảo mật dữ liệu và quyền và lợi ích đối với thông tin cá nhân có thể được bảo vệ đầy đủ và hiệu quả hay không;

đ) Liệu các văn bản pháp luật do bên chuyển dữ liệu và bên nhận ở nước ngoài soạn thảo có quy định đầy đủ trách nhiệm và nghĩa vụ bảo vệ an toàn dữ liệu hay không;

e) Tuân thủ luật pháp, quy định hành chính và quy tắc của Việt Nam;

g) Các vấn đề khác mà cơ quan có thẩm quyền thấy cần thiết để đánh giá.

9. Bên chuyển, xử lý dữ liệu cốt lõi xuyên biên giới định kỳ 6 tháng, bên chuyển, xử lý dữ liệu quan trọng xuyên biên giới định kỳ hàng năm phải thực hiện tự đánh giá rủi ro đối với việc dữ liệu cốt lõi, dữ liệu quan trọng của mình, gửi báo cáo đánh giá rủi ro cho Bộ Công an.

10. Các trường hợp bên chuyển dữ liệu phải thực hiện sửa đổi đánh giá tác động gồm:

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

b) Thay đổi chính sách, quy định bảo vệ an ninh dữ liệu và môi trường an ninh mạng ở quốc gia hoặc khu vực nơi bên nhận lưu trữ dữ liệu, cũng như xảy ra các trường hợp bất khả kháng khác, thay đổi quyền kiểm soát thực tế của bên chuyển dữ liệu hoặc bên nhận dữ liệu ở nước ngoài và các tác động khác đến tính bảo mật của dữ liệu được chuyển;

c) Các trường hợp khác ảnh hưởng đến an ninh an toàn của dữ liệu đã chuyển.

11. Bộ Quốc phòng, Bộ Công an quyết định yêu cầu Bên chuyển dữ liệu ra nước ngoài ngừng chuyển ra nước ngoài, ngừng xử lý ở nước ngoài dữ liệu cốt lõi, dữ liệu quan trọng trong trường hợp:

a) Khi phát hiện dữ liệu được chuyển được sử dụng vào hoạt động vi phạm lợi ích, an ninh quốc gia, lợi ích hợp pháp của tổ chức, cá nhân là chủ thể dữ liệu;

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

c) Để xảy ra sự cố lộ, mất dữ liệu.

# Các hoạt động khác trong xử lý dữ liệu

1. Thu hồi dữ liệu là hoạt động chủ quản dữ liệu lấy lại dữ liệu đã cung cấp, chia sẻ cho các cơ quan, tổ chức, cá nhân, hoặc công khai trên phương tiện truyền thông đại chúng.

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

3. 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.

4. Kết hợp dữ liệu là việc gắn kết dữ liệu từ các nguồn khác nhau vào một tập dữ liệu cho phân tích sau đó hoặc lưu trữ trong kho dữ liệu. Dữ liệu phải được chuẩn hóa trước khi kết hợp.

5. 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.

6. Sao chép dữ liệu là hoạt động truy xuất, tạo lập bản sao của dữ liệu từ dữ liệu gốc. Dữ liệu được sao chép được lưu trữ trên cùng một thiết bị hoặc thiết bị khác và có thể được sử dụng cho các mục đích khác nhau như lưu trữ dự phòng, chia sẻ dữ liệu hoặc phục hồi dữ liệu.

7. Truyền đưa dữ liệu là hoạt động di chuyển dữ liệu qua các kênh truyền, thiết bị lưu trữ hoặc qua các phương thức truyền tải khác.

8. Chuyển giao dữ liệu là hoạt động chuyển quyền sở hữu hoặc quyền sử dụng dữ liệu từ bên có quyền chuyển giao dữ liệu sang bên nhận chuyển giao dữ liệu.

**QUẢN TRỊ, QUẢN LÝ, BẢO VỆ DỮ LIỆU**

# Quản trị, quản lý dữ liệu

1. Trung tâm dữ liệu quốc gia sẽ ban hành Khung quản trị dữ liệu để áp dụng chung cho chủ sở hữu dữ liệu, chủ quản dữ liệu là cơ quan nhà nước có kết nối, chia sẻ với Trung tâm dữ liệu quốc gia.

2. Khuyến nghị các tổ chức, cá nhân áp dụng Khung quản trị dữ liệu do Trung tâm dữ liệu quốc gia ban hành để thuận lợi cho việc kết nối chia sẻ với các cơ quan nhà nước.

3. Xây dựng chính sách dữ liệu là xây dựng chiến lược quản trị dữ liệu bao gồm nguyên tắc, mục tiêu, phạm vi của quản trị dữ liệu, kiến trúc dữ liệu, mô hình dữ liệu, các quy trình chuẩn cho các hoạt động quản lý dữ liệu và các chính sách quản trị cụ thể tương ứng, xây dựng và thống nhất áp dụng các tiêu chuẩn, quy chuẩn cho việc tạo, lưu trữ, sử dụng và chia sẻ dữ liệu.

a) Trung tâm dữ liệu quốc gia xây dựng khung quản trị dữ liệu Trung tâm dữ liệu quốc gia để thống nhất công tác quản trị dữ liệu trên phạm vi cả nước. Chủ quản dữ liệu của các cơ sở dữ liệu của cơ quan nhà nước xây dựng chiến lược quản trị dữ liệu phù hợp với chiến lược dữ liệu quốc gia, chiến lược dữ liệu của Trung tâm dữ liệu quốc gia;

b) Trung tâm dữ liệu quốc gia đề xuất ban hành các tiêu chuẩn, quy chuẩn dữ liệu chia sẻ, thông điệp dữ liệu chia sẻ và điều phối dữ liệu để phục vụ cho việc điều phối và chia sẻ dữ liệu giữa Trung tâm dữ liệu quốc gia và các cơ sở dữ liệu của bộ, cơ quan ngang bộ, cơ quan thuộc chính phủ, Ủy ban nhân dân các tỉnh, thành phố trực thuộc Trung ương; Chủ quản dữ liệu ở các bộ, cơ quan ngang bộ, cơ quan thuộc chính phủ, Ủy ban nhân dân các tỉnh, thành phố trực thuộc Trung ương tuân thủ các tiêu chuẩn;

c) Trung tâm dữ liệu quốc gia là đầu mối thực hiện công tác giám sát việc tuân thủ và bảo đảm chất lượng với dữ liệu ở phạm vi quốc gia và dữ liệu được bộ, cơ quan ngang bộ, cơ quan thuộc chính phủ, Ủy ban nhân dân các tỉnh, thành phố trực thuộc Trung ương chia sẻ; chủ quản dư liệu của bộ, cơ quan ngang bộ, cơ quan thuộc chính phủ, Ủy ban nhân dân các tỉnh, thành phố trực thuộc Trung ương thực hiện giám sát dữ liệu trong phạm vi quản lý của mình.

4. Quản lý lưu trữ dữ liệu bao gồm:

a) Xây dựng hệ thống lưu trữ có khả năng mở rộng, linh hoạt, tin cậy và có dự phòng để đáp ứng nhu cầu lưu trữ hiện tại và tương lai;

b) Theo dõi việc sử dụng dung lượng lưu trữ, dự đoán nhu cầu trong tương lai để lập kế hoạch mở rộng khi cần thiết;

c) Sử dụng các kỹ thuật để tối ưu hóa chi phí và hiệu suất dung lượng lưu trữ;

d) Trách nhiệm của chủ quản cơ sở dữ liệu là bảo đảm hoạt động liên tục của hệ thống lưu trữ và có kế hoạch mở rộng theo nhu cầu một cách tối ưu.

5. Quản lý chất lượng dữ liệu là một quá trình liên tục bảo đảm dữ liệu chất lượng để đáp ứng các yêu cầu nghiệp vụ và cần sự tham gia của tất cả các bên liên quan, bao gồm:

a) Bảo đảm chất lượng dữ liệu về tính chính xác; tính đầy đủ; tính nhất quán; tính hợp lệ; tính kịp thời; tính duy nhất; tính toàn vẹn; tính bảo mật; tính sẵn sàng;

b) Xây dựng và áp dụng các tiêu chuẩn và quy trình chất lượng dữ liệu; đánh giá chất lượng dữ liệu; làm sạch dữ liệu; xây dựng các chỉ số chất lượng dữ liệu;

c) Xây dựng và sử dụng các công cụ để hỗ trợ và phối hợp các hoạt động quản lý chất lượng dữ liệu;

d) Trách nhiệm của chủ quản cơ sở dữ liệu là xây dựng và tuân thủ quy trình bảo đảm chất lượng dữ liệu trong phạm vi quản lý của mình và phối hợp với Trung tâm dữ liệu quốc gia thực hiện giám sát và đối soát dữ liệu chia sẻ.

6. Quản lý các dự án về dữ liệu phải bảo đảm dự án tuân thủ khung quản trị dữ liệu và nguyên tắc quản lý dự án công nghệ thông tin.

7. Quản lý an toàn bảo mật và bảo vệ dữ liệu là các hoạt động xây dựng giải pháp kỹ thuật, quy trình và chính sách nhằm bảo vệ dữ liệu khỏi bị truy cập trái phép, sử dụng sai mục đích, tiết lộ, sửa đổi, phá hủy hoặc mất mát.

a) Xác định và phân loại dữ liệu quan trọng và cốt lõi để có biện pháp bảo vệ tương xứng;

b) Có các biện pháp bảo vệ kiểm soát truy cập dữ liệu; bảo vệ cơ sở dữ liệu; bảo vệ dữ liệu khi truyền; giám sát sử dụng dữ liệu;

c) Có giải pháp chống xâm nhập trái phép để phát hiện và ngăn chặn các cuộc tấn công mạng; và có kế hoạch ứng phó với các sự cố an ninh mạng, bao gồm các bước để ngăn chặn, khắc phục và phục hồi;

d) Trách nhiệm của chủ quản cơ sở dữ liệu là xây dựng và tuân thủ quy trình an toàn bảo mật và bảo vệ dữ liệu trong phạm vi quản lý của mình và phối hợp với Trung tâm dữ liệu quốc gia thực hiện.

8. Quản lý kết nối, tích hợp và chia sẻ dữ liệu bao gồm việc thiết lập và duy trì luồng dữ liệu thông suốt giữa các hệ thống, ứng dụng và người dùng khác nhau để bảo đảm dữ liệu có thể được truy cập, sử dụng và chia sẻ một cách hiệu quả, an toàn và nhất quán.

a) Chủ quản cơ sở dữ liệu quốc gia, cơ sở dữ liệu chuyên ngành phải xác định danh mục dữ liệu cần chia sẻ (danh mục dữ liệu dùng chung, siêu dữ liệu) và dữ liệu khác khi có nhu cầu. Trung tâm dữ liệu quốc gia tổng hợp các danh mục dùng chung và ban hành các chuẩn thông điệp chia sẻ để các bộ, cơ quan ngang bộ, cơ quan thuộc chính phủ, Ủy ban nhân dân các tỉnh, thành phố trực thuộc Trung ương thực hiện chia sẻ dữ liệu;

b) Dữ liệu thống nhất được chia sẻ trên nền tảng điều phối và chia sẻ dữ liệu của Trung tâm dữ liệu quốc gia, và các nền tảng chia sẻ dữ liệu đang hoạt động;

c) Trung tâm dữ liệu quốc gia thiết lập thỏa thuận chia sẻ dữ liệu với chủ quản dữ liệu các cơ sở dữ liệu chuyên ngành của bộ, cơ quan ngang bộ, cơ quan thuộc chính phủ, Ủy ban nhân dân các tỉnh, thành phố trực thuộc Trung ương để xác lập trách nhiệm chia sẻ và khai thác dữ liệu và giám sát quá trình hoạt động chia sẻ, điều phối dữ liệu của các bên liên quan;

d) Chủ quản cơ sở dữ liệu của bộ, cơ quan ngang bộ, cơ quan thuộc chính phủ, Ủy ban nhân dân các tỉnh, thành phố trực thuộc Trung ương chịu trách nhiệm về chất lượng dữ liệu chia sẻ;

9. Quản lý dữ liệu chủ là hoạt quản lý những dữ liệu quan trọng, được sử dụng rộng rãi và ít thay đổi của các thực thể dữ liệu của tổ chức, bao gồm:

a) Xác định dữ liệu chủ. Chủ quản cơ sở dữ liệu quốc gia, cơ sở dữ liệu chuyên ngành phải xác định và công bố dữ liệu chủ trong xây dựng chiến lược quản trị dữ liệu của mình. Trung tâm dữ liệu quốc gia tổng hợp danh sách các dữ liệu chủ và thực hiện quản lý theo danh sách đã được công bố;

b) Trung tâm dữ liệu quốc gia xây dựng chính sách quản lý dữ liệu chủ; xây dựng kho dữ liệu chủ; xây dựng các quy trình cho việc tạo, cập nhật, xóa và sử dụng dữ liệu chủ; xác định rõ các vai trò trách nhiệm cho chất lượng và tính toàn vẹn của dữ liệu chủ; xác định các quy tắc và hướng dẫn cho việc tạo và duy trì dữ liệu chủ; giám sát chất lượng dữ liệu chủ;

c) Chủ quản cơ sở dữ liệu quốc gia, cơ sở dữ liệu chuyên ngành chịu trách nhiệm về chất lượng dữ liệu chủ đã công bố và phối hợp với Trung tâm dữ liệu quốc gia để giám sát, đối soát bảo đảm chất lượng dữ liệu chủ trên toàn hệ thống.

10. Quản lý siêu dữ liệu (đặc tả dữ liệu - metadata) bao gồm các hoạt động tạo lâp, thu thập, lưu trữ, sắp xếp, truy cập, duy trì metadata và sử dụng hiệu quả, bao gồm:

a) Vai trò trách nhiệm quản lý metadata, các yếu tố thành phần trong metadata , sơ đồ metadata và thu thập metadata;

b) Tổ chức danh mục metadata, kho metadata để tổ chức phân loại metadata phục vụ khai thác hiệu quả và cập nhật liên tục;

c) Cơ quan chủ quản cơ sở dữ liệu quốc gia, cơ sở dữ liệu chuyên ngành và các cơ sở dữ liệu khác cần xác định danh mục metadata và quá trình thay đổi metadata để phục vụ công tác nghiệp vụ của mình và chia sẻ với Trung tâm dữ liệu quốc gia;

d) Trung tâm dữ liệu quốc gia tổng hợp xây dựng kho dữ liệu metadata. Phối hợp với bộ, cơ quan ngang bộ, cơ quan thuộc chính phủ, Ủy ban nhân dân các tỉnh, thành phố trực thuộc Trung ương để giám sát và đối soát danh mục metadata.

11. Quản lý truy xuất nguồn gốc dữ liệu là quá trình theo dõi và ghi lại dòng chảy của dữ liệu từ nguồn gốc, lịch xử lý, biến đổi, cho đến đích đến cuối cùng, bao gồm:

a) Xác định, thu thập thông tin về nguồn gốc dữ liệu, thông tin lịch sử quá trình thay đổi dữ liệu;

b) Sử dụng siêu dữ liệu để ghi lại cập nhật và thông tin về nguồn gốc, biến đổi của dữ liệu; tạo mối liên kết giữa dữ liệu và siêu dữ liệu để dễ dàng truy xuất và theo dõi;

c) Sử dụng các công cụ trực quan hoá để xác định nguồn gốc dữ liệu;

d) Cơ quan chủ quản cơ sở dữ liệu quốc gia, cơ sở dữ liệu chuyên ngành và các cơ sở dữ liệu khác cần bảo đảm thông tin xác định nguồn gốc dữ liệu và chia sẻ với Trung tâm dữ liệu quốc gia;

đ) Trung tâm dữ liệu quốc gia sử dụng dữ liệu chia sẻ từ các bộ, cơ quan ngang bộ, cơ quan thuộc chính phủ, Ủy ban nhân dân các tỉnh, thành phố trực thuộc Trung ương được bảo đảm giá trị, kể cả giá trị pháp lý của dữ liệu như dữ liệu từ cơ sở dữ liệu gốc.

12. Quản lý rủi ro và các vấn đề phát sinh khác liên quan đến dữ liệu.

# Xác định 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 pháp luật về quyền riêng tư của dữ liệu trong quá trình xử lý và chuyển giao dữ liệu.

b) Rủi ro an ninh mạng xảy ra do không áp dụng những biện pháp phù hợp giúp bảo vệ những dữ liệu không công khai khỏi những truy cập trái phép từ các đối tượng bên ngoài hoặc thông tin 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 những dữ liệu không được phép công khai khỏi những truy cập trái phép.

d) Rủi ro khác trong xử lý dữ liệu bao gồm: rủi ro vòng đời thông tin xảy ra do việc xử lý những bản ghi dữ liệu không tuân thủ pháp luật và tiêu chuẩn, quy chuẩn, khi vòng đời thay đổi, thì có thể thay đổi giá trị; rủi ro chia sẻ thông tin xảy ra khi không có khả năng duy trì quyền kiểm soát đối với dữ liệu sau khi dữ liệu được chia sẻ cho bên thứ ba; rủi ro quản lý dữ liệu: xảy ra do dữ liệu không chính xác, không đầy đủ, không được cập nhật hoặc thiếu những dữ liệu cần thiết phục vụ việc ra quyết định; gây ra gián đoạn trong quá trình khai thác và sử dụng.

2. Quy định 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 để bảo đảm rằng dữ liệu có thể được khôi phục trong trường hợp mất mát hoặc hỏng hóc. Sao lưu cần được lưu trữ ở một vị trí an toàn và tách biệt với hệ thống chính;

b) Có kế hoạch bảo trì, bảo dưỡng, nâng cấp hệ thống và hệ điều hành nhằm bảo đảm duy trì và cải thiện hiệu suất, tính năng, tính bảo mật và tính nhất quán của hệ thống cơ sở dữ liệu; khi nâng cấp cần có kế hoạch và bảo đảm tính liên tục của dịch vụ; phải có biện pháp ứng phó khôi phục lại hệ thống trong quá trình tiến hành;

c) Thực hiện các biện pháp bảo vệ dữ liệu để không bị truy cập trái phép;

d) Xây dựng, thiết lập các quy tắc chặt chẽ và hạn chế truy cập đối với từng loại dữ liệu, bảo đảm rằng chỉ những người dùng có nhiệm vụ liên quan đến dữ liệu đó hoặc được sự đồng ý của cơ quan chủ quản dữ liệu mới có thể truy cập được vào những dữ liệu có thông tin nhạy cảm;

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 như tường lửa, phần mềm diệt virus, chống phần mềm độc hại để bảo vệ hệ thống khỏi các mối đe dọa;

g) Thực hiện đánh giá rủi ro định kỳ để xác định các điểm yếu trong hệ thống và áp dụng các biện pháp giảm thiểu rủi ro tương ứng;

h) Xây dựng phương án, kế hoạch xử lý sự cố dữ liệu để bảo đảm cơ quan, tổ chức có thể nhanh chóng ứng phó, khắc phục sự cố và hoạt động bình thường sau khi xảy ra các sự cố như tấn công mạng, mất dữ liệu hoặc hỏng hóc thiết bị;

i) Đào tạo nhân viên về các biện pháp bảo mật dữ liệu, cách nhận biết các mối đe dọa, cách xử lý khi phát hiện rủi ro bảo mật; huấn luyện, diễn tập, phòng ngừa sự cố, giám sát phát hiện, bảo đảm các điều kiện sẵn sàng khi có sự cố;

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

# Bảo vệ dữ liệu

1. Cơ quan, tổ chức, cá nhân phải tuân thủ quy định pháp luật về dữ liệu, pháp luật về giao dịch điện tử, pháp luật về an toàn thông tin mạng, pháp luật về an ninh mạng và quy định khác của pháp luật có liên quan khi xử lý dữ liệu.

2. Dữ liệu là bí mật nhà nước phải tuân thủ quy định pháp luật về bảo vệ bí mật nhà nước và pháp luật về cơ yếu.

3. Việc bảo vệ dữ liệu cá nhân tuân thủ theo quy định pháp luật về bảo vệ dữ liệu cá nhân.

4. Việc bảo vệ dữ liệu phải tuân thủ các chính sách chung về an ninh quốc phòng; các cơ quan nhà nước phải thực hiện nhiệm vụ quản lý, bảo vệ dữ liệu trong ngành, lĩnh vực do mình quản lý; thiết lập hệ thống bảo vệ dữ liệu thống nhất, có hiệu quả cao và có thẩm quyền để đánh giá rủi ro an ninh dữ liệu, báo cáo, chia sẻ thông tin, giám sát và cảnh báo sớm. Nhà nước bảo hộ quyền, lợi ích của cá nhân, tổ chức về dữ liệu; khuyến khích sử dụng dữ liệu hợp pháp, hợp lý, hiệu quả; bảo đảm dữ liệu được lưu thông tự do, hợp pháp, có trật tự; thúc đẩy phát triển nền kinh tế số lấy dữ liệu làm yếu tố then chốt. Khuyến khích các chủ quản dữ liệu khác xây dựng các quy định riêng về bảo vệ dữ liệu do mình quản lý.

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

a) Biện pháp quản lý có liên quan tới xử lý dữ liệu: Xây dựng chính sách, quy chế đánh giá an ninh dữ liệu, bảo đảm an toàn thông tin, bảo mật dữ liệu, ứng phó sự cố, bảo đảm tuân thủ các quy định 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 tới 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 pháp luật;

c) Biện pháp quản lý nhân lực bảo vệ dữ liệu: Quy chế quản lý con người, đào tạo nhân lực bảo vệ dữ liệu;

d) Biện pháp bảo vệ dữ liệu do cơ quan quản lý nhà nước có thẩm quyền thực hiện theo quy định pháp luật;

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

# Xây dựng và tổ chức thực hiện chính sách, quy định bảo vệ dữ liệu

1. Chủ sở hữu dữ liệu, chủ quản dữ liệu là cơ quan nhà nước phải chịu trách nhiệm về bảo mật cho hoạt động xử lý dữ liệu, thực hiện bảo vệ phân cấp đối với tất cả các loại dữ liệu, trong trường hợp các cấp dữ liệu khác nhau được xử lý cùng một lúc và khó áp dụng các biện pháp bảo vệ riêng biệt thì phải thực hiện các biện pháp bảo vệ theo yêu cầu của cấp cao nhất, để bảo đảm dữ liệu tiếp tục ở trạng thái bảo vệ hiệu quả và sử dụng hợp pháp

2. Chủ quản dữ liệu phải phân loại dữ liệu, xác định dữ liệu quan trọng, dữ liệu cốt lõi theo danh mục dữ liệu cốt lõi, dữ liệu quan trọng do Thủ tướng Chính phủ ban hành và tạo thành một danh mục cụ thể cho đơn vị đó.

# Quản lý bảo vệ dữ liệu trong quá trình xử lý

1. Chủ quản dữ liệu thiết lập hệ thống quản lý bảo vệ cho toàn bộ vòng đời của dữ liệu, đồng thời soạn thảo các yêu cầu bảo vệ phân cấp cụ thể và quy trình vận hành để thu thập, lưu trữ, sử dụng, xử lý, truyền, cung cấp và các hoạt động khác cho các cấp độ dữ liệu khác nhau.

2. Chủ quản dữ liệu thực hiện các biện pháp bảo vệ dữ liệu trong quá trình thu thập, tạo lập dữ liệu theo phân cấp. Trường hợp thu thập, tạo lập dữ liệu cốt lõi, dữ liệu quan trọng, chủ quản dữ liệu cần:

a) Xây dựng quy trình thu thập, tạo lập dữ liệu, làm rõ mục đích, quy mô, phương pháp, phạm vi, loại hình, thời gian lưu trữ, vị trí lưu trữ của việc thu thập dữ liệu, cũng như định dạng dữ liệu, tiêu chí chất lượng, phương pháp đánh giá và các yêu cầu khác;

b) Tiến hành đánh giá bảo vệ trước khi thu thập, bao gồm xem mục đích, phạm vi, tần suất, phương pháp, thời gian lưu trữ của việc thu thập dữ liệu có tuân thủ luật pháp và quy định hay không;

c) Kiểm tra tính xác thực, chính xác của dữ liệu, thường xuyên phân tích, giám sát chất lượng dữ liệu, cảnh báo và khắc phục kịp thời những dữ liệu bất thường;

d) Theo dõi, ghi lại quá trình thu thập dữ liệu để bảo đảm truy xuất nguồn gốc hoạt động thu thập dữ liệu.

3. Chủ quản dữ liệu có trách nhiệm lưu trữ dữ liệu theo phương pháp, thời hạn theo quy định của pháp luật. Trường hợp dữ liệu được lưu trữ là dữ liệu cốt lõi, dữ liệu quan trọng, chủ quản dữ liệu cần:

a) Xây dựng hệ thống quản lý lưu trữ dữ liệu quan trọng và quy định các hệ thống bảo vệ an ninh, quy trình truy cập;

b) Triển khai các biện pháp kỹ thuật, quản lý an toàn dữ liệu quan trọng và đánh giá thường xuyên gồm sử dụng công nghệ mã hóa để bảo vệ tính bảo vệ và toàn vẹn của dữ liệu quan trọng; cung cấp các biện pháp cách ly hợp lý giữa mạng thông tin công cộng và hệ thống lưu trữ; thiết lập hệ thống quản lý chặt chẽ đối với nhân viên vận hành và bảo trì nơi chứa dữ liệu quan trọng và tiến hành kiểm tra lý lịch bảo vệ đối với tất cả nhân viên vận hành và bảo trì;

c) Trường hợp dữ liệu cốt lõi, dữ liệu quan trọng có thời gian bảo quản cụ thể, trước khi hết thời hạn, chủ quản dữ liệu phải kịp thời thực hiện các thao tác như truyền, giải mã dữ liệu liên quan và điều chỉnh các biện pháp bảo vệ dữ liệu liên quan tùy theo tình hình; áp dụng các công cụ, biện pháp kỹ thuật phù hợp để tiêu hủy kịp thời những dữ liệu quan trọng đã quá thời hạn lưu trữ hoặc không còn cần thiết cho mục đích xử lý;

d) Xây dựng kế hoạch sao lưu, phục hồi dữ liệu quan trọng, làm rõ phạm vi, tần suất, công cụ, quy trình, thông số kỹ thuật ghi nhật ký, thời gian lưu trữ dữ liệu của việc sao lưu và phục hồi;

đ) Sử dụng các công cụ, biện pháp kỹ thuật như công cụ tự động hóa, sao lưu ngoại vi để tự động thực hiện các hoạt động liên quan đến sao lưu, phục hồi theo chiến lược đã thiết lập và ghi lại quá trình sao lưu, phục hồi dữ liệu;

e) Thường xuyên rà soát tính sẵn sàng, tính toàn vẹn và tính nhất quán của dữ liệu sao lưu, đánh giá chất lượng phục hồi dữ liệu và có biện pháp xử lý.

4. Chủ quản dữ liệu cần thực hiện các việc sau khi xử lý, sử dụng dữ liệu cốt lõi, dữ liệu quan trọng:

a) Xây dựng và triển khai các chính sách và hệ thống kiểm soát truy cập đối với các dữ liệu quan trọng, tuân thủ các nguyên tắc đặc quyền tối thiểu, phân chia nhiệm vụ và thực hiện các biện pháp bảo vệ an ninh;

b) Thiết lập nền tảng quản lý truy cập và nhận dạng thống nhất, áp dụng các biện pháp kỹ thuật như xác thực đa yếu tố và quản lý mật khẩu, cung cấp và triển khai các cơ chế kiểm soát truy cập chi tiết đối với các dữ liệu quan trọng, hạn chế phạm vi dữ liệu mà người dùng có thể truy cập, ngăn chặn việc truy cập trái phép dữ liệu;

c) Hạn chế nghiêm ngặt việc thiết lập và sử dụng các tài khoản đặc quyền trong hệ thống chứa dữ liệu quan trọng;

d) Sử dụng các công nghệ phù hợp để kiểm soát mục đích, phạm vi sử dụng dữ liệu quan trọng và giảm nguy cơ rò rỉ dữ liệu.

5. Chủ quản dữ liệu có trách nhiệm làm rõ phạm vi, chủng loại, yêu cầu, thủ tục, soạn thảo chính sách bảo mật và áp dụng các biện pháp bảo vệ dựa trên loại, mức độ và tình huống ứng dụng của dữ liệu được cung cấp ra bên ngoài.

6. Chủ quản dữ liệu phải phân tích, đánh giá tác động có thể ảnh hưởng đến an ninh quốc gia, lợi ích công cộng trước khi công bố dữ liệu, nếu có tác động lớn thì không được tiết lộ.

7. Chủ quản dữ liệu phải thiết lập hệ thống xóa, hủy dữ liệu, làm rõ các yêu cầu như mục tiêu, quy tắc, quy trình, kỹ thuật xóa, hủy, ghi nhận và lưu giữ hoạt động xóa, hủy. Trường hợp cá nhân, tổ chức yêu cầu xóa, hủy theo quy định của pháp luật, thỏa thuận hợp đồng thì chủ quản dữ liệu có trách nhiệm xóa, hủy dữ liệu tương ứng.

Khi xóa, hủy dữ liệu cốt lõi, dữ liệu quan trọng, chủ quản dữ liệu cần:

a) Xây dựng các thông số vận hành xóa, hủy dữ liệu và thực hiện các hoạt động xóa, hủy dữ liệu quan trọng theo đúng đặc tả vận hành;

b) Thiết lập các thủ tục đánh giá và phê duyệt việc xóa dữ liệu quan trọng, đánh giá phạm vi dữ liệu quan trọng cần xóa, lý do xóa, khả năng sử dụng lại và thực hiện xóa dữ liệu sau khi được nhân viên an toàn dữ liệu của tổ chức phê duyệt;

c) Cung cấp các biện pháp kỹ thuật và công cụ xóa dữ liệu để xóa dữ liệu quan trọng và các bản sao của dữ liệu sau khi được phê duyệt, bao gồm dữ liệu dự phòng, dữ liệu phái sinh và dữ liệu nhật ký vận hành trong quá trình xử lý dữ liệu, bảo đảm dữ liệu đã xóa không thể phục hồi được bằng các phương tiện thương mại,

d) Thiết lập cơ chế đánh giá tác động xóa dữ liệu và thường xuyên kiểm tra hiệu quả của các biện pháp xóa;

đ) Ghi lại nhật ký quá trình xóa dữ liệu, ghi lại quá trình phê duyệt và thực hiện xóa dữ liệu và các trường hợp cụ thể của dữ liệu bị xóa;

e) Cập nhật kịp thời danh sách, thư mục dữ liệu quan trọng sau khi xóa dữ liệu.

8. Trường hợp chủ quản dữ liệu có nhu cầu chuyển dữ liệu vì các lý do như sáp nhập, tổ chức lại, phá sản thì phải làm rõ kế hoạch chuyển dữ liệu và thông báo cho người dùng bị ảnh hưởng thông qua các phương thức như điện thoại, tin nhắn văn bản, email, thông báo.

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 quan trọng, tên hoặc thông tin liên lạc của bên tiếp nhận cho các cơ quan có thẩm quyền có liên quan.

9. Trường hợp chủ quản dữ liệu ủy thác cho người 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 các phương thức như ký kết hợp đồng, thỏa thuận. Trường hợp ủy thác xử lý dữ liệu quan trọng, dữ liệu cốt lõi thì tiến hành xác minh năng lực, trình độ bảo vệ an ninh dữ liệu của bên được ủy thác.

10. Chủ quản dữ liệu phải ghi nhật ký xử lý dữ liệu, quản lý thẩm quyền, hoạt động của nhân sự, trong toàn bộ vòng đời của quá trình xử lý dữ liệu. Nhật ký được lưu giữ 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 của mình. 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 an ninh dữ liệu và việc triển khai chúng, các biện pháp kỹ thuật như mã hóa, sao lưu, dán nhãn, kiểm soát truy cập và xác thực bảo vệ, cũng như các biện pháp cần thiết khác và hiệu quả của chúng;

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

đ) Đánh giá rủi ro đối với dữ liệu quan trọng được cung cấp, ủy thác xử lý;

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

# 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 làm rõ người chịu trách nhiệm về bảo vệ dữ liệu và bộ phận có chức năng bảo vệ an toàn dữ liệu.

2. Người chịu trách nhiệm về bảo vệ dữ liệu có trách nhiệm quản lý, bảo vệ 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; phải có kiến thức chuyên môn về an toàn dữ liệu và kinh nghiệm làm việc quản lý có liên quan; thực hiện báo cáo trực tiếp về tình hình an toàn dữ liệu cho các cơ quan có thẩm quyền theo quy định

3. Bộ phận có chức năng bảo vệ an toàn dữ liệu có trách nhiệm sau đây:

a) Phát triển, triển khai hệ thống quản lý an toàn dữ liệu, quy trình vận hành, kế hoạch ứng cứu khẩn cấp sự cố an toàn 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 đề xuất ra quyết định quan trọng liên quan đến bảo vệ dữ liệu cốt lõi, dữ liệu quan trọng;

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

4. Chủ sở hữu dữ liệu, chủ quản dữ liệu cốt lõi, dữ liệu quan trọng phải thực hiện quản lý nhân sự có liên quan đến dữ liệu cốt lõi, dữ liệu quan trọng

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) Tiến hành kiểm tra lý lịch bảo vệ đối với người phụ trách bộ phận có chức năng bảo vệ an toàn dữ liệu và nhân sự chủ chốt trước khi tuyển dụng;

c) Thường xuyên đánh giá nhân sự xử lý dữ liệu cốt lõi, dữ liệu quan trọng và xác định trình độ chuyên môn dựa trên kết quả đánh giá;

d) Ký thỏa thuận trách nhiệm bảo mật với nhân viên xử lý dữ liệu quan trọng;

đ) Khi nhân viên xử lý dữ liệu dừng công việc, chủ sở hữu dữ liệu, chủ quản dữ liệu phải ký thỏa thuận bảo mật để bảo đảm rằng nhân viên tiếp tục thực hiện nghĩa vụ bảo mật của mình trong khoảng thời gian hợp lý sau khi chuyển đi.

5. Chủ sở hữu dữ liệu, chủ quản dữ liệu thực hiện công tác đào tạo nhân sự bảo vệ dữ liệu:

a) Xây dựng kế hoạch đào tạo về an toàn dữ liệu hàng năm, làm rõ nội dung đào tạo, thời gian đào tạo và yêu cầu đào tạo. Nội dung đào tạo bao gồm nhưng không giới hạn các quy định pháp luật, tiêu chuẩn chính sách, thực tiễn kỹ thuật, nhận thức về bảo vệ liên quan đến bảo vệ dữ liệu quan trọng;

b) Thực hiện đào tạo hàng năm theo kế hoạch đào tạo và đánh giá, phân loại, ghi nhận, lưu trữ kết quả đào tạo;

c) Kịp thời điều chỉnh hoặc cập nhật thường xuyên kế hoạch đào tạo theo tình hình thực tế.

# Giám sát bảo mật dữ liệu, cảnh báo sớm và quản lý khẩn cấp

1. Bộ Công an thiết lập cơ chế giám sát rủi ro an toàn dữ liệu, tổ chức soạn thảo các giao diện, 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.

2. 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 cơ quan dịch vụ bảo mật, tổ chức nghiên cứu khoa học thực hiện báo cáo, chia sẻ thông tin rủi ro an toàn dữ liệu.

Bộ ngành, địa phương 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 cho Bộ Công an.

Chủ quản dữ liệu phải báo cáo kịp thời cho Bộ ngành, địa phương quản lý về những rủi ro có thể gây ra sự cố an ninh.

3. 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.

Bộ ngành, địa phương tổ chức riêng và thực hiện các nỗ lực ứng phó khẩn cấp đối với các sự cố bảo mật dữ liệu trong phạm vi quản lý. Các sự cố bảo mật liên quan đến dữ liệu quan trọng, dữ liệu cốt lõi phải được báo cáo ngay cho Bộ Công an về việc phát triển và xử lý sự cố.

4. Chủ quản dữ liệu thực hiện diễn tập kế hoạch dự phòng đối với các sự cố an toàn dữ liệu quan trọng, tiến hành diễn tập khẩn cấp thường xuyên, 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;

Sau khi xảy ra sự cố an toàn dữ liệu, chủ quản 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 ngành, địa phương quản lý trong thời gian sớm nhất có thể, đồng thời lập báo cáo tóm tắt sau khi sự cố hoàn thành và báo cáo việc xử lý sự cố an toàn dữ liệu cho Bộ ngành, địa phương quản lý hàng năm.

5. Chủ quản dữ liệu có trách nhiệm thông báo kịp thời cho cá nhân, tổ chức liên quan 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.

# Yêu cầu khi cung cấp, ủy thác xử lý dữ liệu cốt lõi, dữ liệu quan trọng trong nước

1. Trước khi thực hiện cung cấp, ủy thác xử lý dữ liệu cốt lõi, dữ liệu quan trọng cho tổ chức, cá nhân khác trong nước, chủ quản dữ liệu phải tiến hành đánh giá rủi ro, trừ trường hợp đó là việc thực hiện nhiệm vụ hoặc nghĩa vụ theo quy định của pháp luật. Việc đánh giá rủi ro phải tập trung vào các yếu tố sau:

a) Việc cung cấp, ủy thác xử lý dữ liệu cũng như mục đích, phương pháp và phạm vi xử lý dữ liệu cốt lõi, dữ liệu quan trọng của bên nhận dữ liệu có hợp pháp, phù hợp và cần thiết hay không;

b) Nguy cơ dữ liệu cốt lõi, dữ liệu quan trọng được cung cấp, ủy thác xử lý bị giả mạo, phá hủy, rò rỉ hoặc bị thu thập, sử dụng, chia sẻ trái phép, cũng như rủi ro đối với an ninh quốc gia, lợi ích công cộng, quyền và lợi ích hợp pháp của cá nhân, tổ chức;

c) Tính liêm chính, tình trạng tuân thủ pháp luật, mối quan hệ hợp tác với các cơ quan chính phủ, tổ chức, cá nhân nước ngoài của bên nhận dữ liệu;

d) Liệu các yêu cầu về an toàn dữ liệu trong các hợp đồng liên quan được ký kết hoặc soạn thảo với bên nhận dữ liệu có thể ràng buộc hiệu quả việc thực hiện nghĩa vụ bảo vệ an toàn dữ liệu của bên nhận dữ liệu hay không;

đ) Liệu các biện pháp kỹ thuật và quản lý được sử dụng hoặc đề xuất sử dụng có thể ngăn ngừa hiệu quả các rủi ro như thay đổi, phá hủy hoặc rò rỉ hoặc thu thập, sử dụng, chia sẻ dữ liệu trái phép hay không;

e) Các nội dung đánh giá khác do các cơ quan có thẩm quyền có liên quan quy định.

2. 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 khác khác thì phải 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.

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

Trường hợp hai hoặc nhiều chủ quản dữ liệu cùng quyết định mục đích, phương pháp xử lý dữ liệu cốt lõi, dữ liệu quan trọng thì phải thỏa thuận về quyền và nghĩa vụ tương ứng.

3. Khi thực hiện cung cấp, chuyển giao dữ liệu quan trọng, chủ quản dữ liệu cần:

a) Thiết lập kênh bảo vệ và thực hiện xác thực nhận dạng chủ thể ở cả hai đầu kênh truyền;

b) Thực hiện mã hóa, chữ ký, chống phát lại và các biện pháp khác để bảo đảm tính bí mật, toàn vẹn và không thể chối bỏ dữ liệu trong quá trình truyền tải;

c) Bảo vệ an ninh mạng và thực hiện cách ly an ninh giữa các vùng mạng hoặc miền bảo vệ khác nhau;

d) Cung cấp hệ thống quản lý khóa để quản lý việc tạo, lưu trữ, sử dụng, phân phối, cập nhật và hủy khóa;

đ) Giám sát việc thực hiện nghĩa vụ bảo vệ an toàn của người tiếp nhận.

**TRUNG TÂM DỮ LIỆU QUỐC GIA,**

**CƠ SỞ DỮ LIỆU TỔNG HỢP QUỐC GIA**

# Cơ sở hạ tầng của Trung tâm dữ liệu quốc gia

1. Trung tâm dữ liệu quốc gia được thiết kế, xây dựng đáp ứng các yêu cầu kỹ thuật, tiêu chuẩn, quy chuẩn, định mức về trung tâm dữ liệu trong nước và quốc tế, phù hợp với quy hoạch hạ tầng thông tin và truyền thông, bảo đảm chống bom đạn, khủng bố, thiên tai; tiêu chuẩn, yêu cầu về bảo vệ môi trường, ưu tiên sử dụng các nguồn năng lượng tái tạo, giải pháp thông minh để kiểm soát nguồn năng lượng.

2. Hệ thống công nghệ thông tin của Trung tâm dữ liệu quốc gia được thiết kế xây dựng đáp ứng các yêu cầu kỹ thuật, tiêu chuẩn, quy chuẩn kỹ thuật về bảo đảm mức độ sẵn sàng của hệ thống, thiết kế hệ thống với mức dự phòng nhằm sẵn sàng trong trường hợp mở rộng khi cần thiết. Môi trường vận hành hệ thống thông tin của Trung tâm dữ liệu quốc gia tách biệt với các môi trường 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.

3. Các thành phần công nghệ thông tin chính của Trung tâm dữ liệu quốc gia gồm:

a) Nền tảng chia sẻ, điều phối dữ liệu;

b) Cơ sở hạ tầng điện toán đám mây;

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 Đảng, Nhà nước, tổ chức chính trị - xã hội, bảo đảm việc phát triển các phân hệ tích hợp, đồng bộ, khai thác dữ liệu, yêu cầu cao về bảo mật thông tin;

c) Cơ sở dữ liệu tổng hợp quốc gia;

Cơ sở dữ liệu tổng hợp quốc gia được xây dựng theo tiêu chuẩn, quy chuẩn kỹ thuật công nghệ thông tin, định mức kinh tế - kỹ thuật, bảo đảm hoạt động ổn định, liên tục; bảo đảm an ninh, an toàn thông tin, bảo vệ dữ liệu cá nhân, thuận lợi cho việc thu thập, cập nhật, điều chỉnh, khai thác, sử dụng; bảo đảm kết nối, chia sẻ, quyền khai thác thông tin với các cơ sở dữ liệu quốc gia, cơ sở dữ liệu chuyên ngành, cơ sở dữ liệu khác và hệ thống thông tin khác.

d) Hệ thống phân tích dữ liệu phục vụ công tác quản lý;

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.

đ) Cổng dịch vụ công quốc gia;

e) Hệ thống, phần mềm quản lý, khai thác, cung cấp dịch vụ dữ liệu, cổng dữ liệu mở, cổng dịch vụ dữ liệu có thu phí.

4. Cơ quan nhà nước, tổ chức chính trị - xã hội sử dụng hạ tầng của Trung tâm dữ liệu quốc gia hoặc đầu tư hạ tầng đặt tại Trung tâm dữ liệu quốc gia khi đáp ứng các quy định về tiêu chuẩn, quy chuẩn kỹ thuật của trung tâm dữ liệu.

5. Cơ quan nhà nước, tổ chức chính trị - xã hội có nhu cầu sử dụng hạ tầng tại Trung tâm dữ liệu quốc gia 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 đặt hạ tầng thiết bị hay sử dụng hạ tầng của Trung tâm dữ liệu quốc gia; quy mô hệ thống dự kiến đặt tại Trung tâm dữ liệu quốc gia (số rack); nhu cầu về nhân lực hỗ trợ quản trị, vận hành hạ tầng, hệ thống thông tin.

# Trách nhiệm của Trung tâm dữ liệu quốc gia

1. Trung tâm dữ liệu quốc gia tích hợp, đồng bộ, lưu trữ, phân tích, khai thác dữ liệu của các cơ quan Đảng, Nhà nước, tổ chức chính trị - xã hội theo quy định pháp luật nhằm tạo lập, quản trị Cơ sở dữ liệu tổng hợp quốc gia.

2. Trung tâm dữ liệu quốc gia quản trị, vận hành hạ tầng kỹ thuật, hạ tầng công nghệ thông tin tại Trung tâm dữ liệu quốc gia; cung cấp hạ tầng kỹ thuật, hạ tầng công nghệ thông tin cho cơ quan Nhà nước, tổ chức chính trị - xã hội có nhu cầu sử dụng để khai thác, vận hành, nâng cao hiệu quả, bảo đảm an ninh, an toàn thông tin.

3. Tổ chức vận hành, quản trị, lưu trữ, quản lý, khai thác, điều phối dữ liệu của Trung tâm dữ liệu quốc gia để thực hiện các công tác quản lý nhà nước; phân tích phục vụ điều hành, xây dựng chính sách; nghiên cứu phát triển dữ liệu.

4. Trung tâm dữ liệu quốc gia thực hiện nâng cấp, bảo trì, sửa chữa hạ tầng, thiết bị do Trung tâm dữ liệu quốc gia đầu tư, trang bị. Cơ quan Nhà nước, tổ chức chính trị - xã hội thực hiện nâng cấp, bảo trì, sửa chữa hạ tầng, thiết bị do cơ quan, tổ chức đó đầu tư và đặt tại Trung tâm dữ liệu quốc gia.

5. Hướng dẫn cơ quan nhà nước, tổ chức chính trị - xã hội trong việc áp dụng các tiêu chuẩn chất lượng dữ liệu.

6. Thực hiện các biện pháp giám sát, đánh giá chất lượng dữ liệu của các cơ quan, tổ chức, cá nhân đối với dữ liệu đồng bộ về Trung tâm dữ liệu quốc gia.

7. Xây dựng quy trình, quy chế quản lý hoạt động điều phối dữ liệu giữa Cơ sở dữ liệu tổng hợp quốc gia và các cơ sở dữ liệu quốc gia, cơ sở dữ liệu chuyên ngành; Xây dựng hệ thống chỉ số đo lường và đánh giá hiệu suất quản trị dữ liệu.

8.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, bao gồm:

a) Biện pháp quản lý: Xây dựng chính sách, quy chế đánh giá an ninh dữ liệu, bảo đảm an toàn thông tin, bảo mật dữ liệu, ứng phó sự cố, bảo đảm tuân thủ các quy định bảo vệ dữ liệu và các biện pháp quản lý khác theo quy định của pháp luật;

b) Biện pháp kỹ thuật: 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 pháp luật;

c) Biện pháp quản lý nhân lực bảo vệ dữ liệu: Quy chế quản lý con người, đào tạo nhân lực bảo vệ dữ liệu;

d) Biện pháp bảo vệ dữ liệu do cơ quan quản lý nhà nước có thẩm quyền thực hiện theo quy định pháp luật;

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

9. 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.

# Bảo đảm nguồn lực xây dựng, phát triển Trung tâm dữ liệu quốc gia

1. Trung tâm dữ liệu quốc gia xây dựng và thực hiện kế hoạch, chương trình đào tạo, nâng cao chất lượng nguồn nhân lực phục vụ quản trị, vận hành cho các cán bộ của Trung tâm dữ liệu quốc gia. Phát triển các hình thức liên kết đào tạo nhằm đáp ứng tốt nhu cầu và nâng cao chất lượng nguồn nhân lực.

2. Trung tâm dữ liệu quốc gia xây dựng cơ chế sử dụng nguồn thu phí, lệ phí và nguồn thu sự nghiệp để hỗ trợ chi trả chế độ bồi dưỡng chính sách cho cán bộ Trung tâm dữ liệu quốc gia theo quy định của pháp luật.

3. Tăng cường hợp tác quốc tế, thúc đẩy quan hệ với các cơ sở đào tạo, tổ chức quốc tế để xây dựng các chương trình đào tạo, tập huấn nâng cao năng lực cho cán bộ công tác tại Trung tâm dữ liệu quốc gia.

4. Xây dựng chính sách thu hút, trọng dụng, cơ chế đãi ngộ nguồn nhân lực chất lượng cao ở khu vực ngoài nhà nước.

# Khai thác và sử dụng cơ sở dữ liệu tổng hợp quốc gia

1. Cơ sở dữ liệu tổng hợp quốc gia được Chính phủ xây dựng và quản lý tập trung, thống nhất tại Trung tâm dữ liệu quốc gia. Dữ liệu được thu thập, cập nhật, đồng bộ vào Cơ sở dữ liệu tổng hợp quốc gia theo khoản 1, 2 điều 34 Luật Dữ liệu. Cơ sở dữ liệu tổng hợp quốc gia được xây dựng phục vụ việc khai thác, sử dụng chung đáp ứng hoạt động của cơ quan Đảng, Nhà nước, Ủy ban Mặt trận Tổ quốc Việt Nam, các tổ chức chính trị - xã hội và các tổ chức cá nhân có nhu cầu.

2. Để bảo đảm các sản phẩm, dịch vụ của cơ sở dữ liệu tổng hợp quốc gia có giá trị pháp lý, dữ liệu trong Cơ sở dữ liệu tổng hợp quốc gia phải có giá trị khai thác và sử dụng như dữ liệu gốc. Các hoạt động bảo đảm giá trị gồm:

a) Cơ quan chủ quản các cơ sở dữ liệu nguồn cung cấp chia sẻ dữ liệu cho cơ sở dữ liệu quốc gia trực tiếp qua chia sẻ dữ liệu hoặc gián tiếp thông qua các dịch vụ công phải bảo đảm giá trị dữ liệu chia sẻ có giá trị như giá trị gốc;

b) Mọi thay đổi tại cơ sở dữ liệu nguồn phải được cập nhật kịp thời lên cơ sở dữ liệu quốc gia bảo đảm tính nhất quán của dữ liệu sử dụng trên toàn hệ thống bao gồm Cơ sở dữ liệu tổng hợp quốc gia và các cơ sở dữ liệu của bộ, cơ quan ngang bộ, cơ quan thuộc chính phủ, Ủy ban nhân dân các tỉnh, thành phố trực thuộc Trung ương;

c) Dữ liệu được hình thành tại Trung tâm dữ liệu quốc gia trong quá trình phân tích tổng hợp dữ liệu từ cơ sở dữ liệu tổng hợp quốc gia cũng như từ quá trình nghiên cứu từ nguồn dữ liệu mở trong và ngoài nước khi đã được lưu trữ như trong Cơ sở dữ liệu tổng hợp quốc gia được coi có giá trị gốc để khai thác sử dụng.

3. Cơ sở dữ liệu tổng hợp quốc gia phục vụ quản lý điều hành Chính phủ và Thủ tướng chính phủ bao gồm và không giới hạn:

a) Xây dựng, phát triển bộ chỉ số phục vụ hoạt động điều hành của Chính phủ và Thủ tướng chính phủ dựa trên dữ liệu;

b) Phân tích tổng hợp dữ liệu từ cơ sở dữ liệu quốc gia hỗ trợ việc ra quyết định. Phân tích dữ liệu về các lĩnh vực liên quan đến con người, thủ tục hành chính, dữ liệu về kinh tế và các lĩnh vực khác;

4. Cơ sở dữ liệu tổng hợp quốc gia phục vụ bộ, cơ quan ngang bộ, cơ quan thuộc chính phủ, Ủy ban nhân dân các tỉnh, thành phố trực thuộc Trung ương bao gồm và không giới hạn các nội dung sau:

a) Bảo đảm cung cấp các dữ liệu dùng chung một cách chính xác kịp thời để thực hiện các dịch vụ công cho người dân và doanh nghiệp;

b) Cung cấp công cụ và dịch vụ phân tích tổng hợp dữ liệu từ cơ sở dữ liệu tổng hợp quốc gia trong phạm vi của địa phương hoặc trong phạm vi vùng kinh tế để phục vụ công tác chỉ đạo điều hành của địa phương đối với các dữ liệu về tình hình kinh tế; an sinh xã hội, bảo hiểm y tế, giáo dục; lao động, việc làm, tình trạng thất nghiệp; môi trường, biến đổi khí hậu; an ninh trật tự, tội phạm và các dữ liệu khác;

5. Cơ sở dữ liệu tổng hợp quốc gia phục vụ theo yêu cầu cụ thể cơ quan Đảng, Ủy ban Mặt trận Tổ quốc Việt Nam và các tổ chức chính trị - xã hội các dữ liệu.

6. Cơ sở dữ liệu tổng hợp quốc gia phục vụ tổ chức, cá nhân thông qua cổng dịch vụ công, cổng dữ liệu mở và các dịch vụ phân tích tổng hợp khác phù hợp với quy định của pháp luật.

7. Phương thức khai thác cơ sở dữ liệu tổng hợp quốc gia:

a) Các hệ thống thông tin cơ sở dữ liệu của bộ, cơ quan ngang bộ, cơ quan thuộc chính phủ, Ủy ban nhân dân các tỉnh, thành phố trực thuộc Trung ương kết nối chia sẻ dữ liệu thông qua Nền tảng chia sẻ, điều phối dữ liệu của Trung tâm dữ liệu quốc gia;

b) Các hệ thống tin của tổ chức, cá nhân kết nối chia sẻ dữ liệu thông qua cổng dữ liệu của Trung tâm dữ liệu quốc gia;

c) Trung tâm dữ liệu quốc gia có trách nhiệm cung cấp và hướng dẫn đầy đủ thông tin quy trình thực hiện kết nối, tích hợp, điều phối và chia sẻ dữ liệu.

# Kết nối, chia sẻ dữ liệu với Cơ sở dữ liệu tổng hợp quốc gia

1. Tiêu chuẩn, quy chuẩn kết nối chia sẻ

a) Tiêu chuẩn kết nối chia sẻ dữ liệu là tập hợp các quy tắc, hướng dẫn, quy định kỹ thuật được thiết lập nhằm bảo đảm việc chia sẻ dữ liệu giữa các cơ sở dữ liệu được thống nhất, nhanh, hiệu quả, đơn giản hóa quy trình kết nối chia sẻ, thúc đẩy quá trình chuyển đổi số;

b) Trung tâm dữ liệu quốc gia có trách nhiệm hướng dẫn thống nhất áp dụng các tiêu chuẩn, quy chuẩn, thông điệp dữ liệu cho việc kết nối và chia sẻ dữ liệu cho các cơ sở dữ liệu quốc gia, cơ sở dữ liệu chuyên ngành và các cơ sở dữ liệu khác;

c) Chủ quản các cơ sở dữ liệu của các cơ quan nhà nước khi xây dựng cơ sở dữ liệu có trách nhiệm tuân thủ hướng dẫn của Trung tâm dữ liệu quốc gia để bảo đảm việc kết nối, chia sẻ dữ liệu được thực hiện thông qua một nền tảng thống nhất;

d) Khuyến khích các tổ chức, cá nhân áp dụng các tiêu chuẩn, quy chuẩn kỹ thuật để bảo đảm khả năng sẵn sàng kết nối chia sẻ với cơ quan nhà nước khi có yêu cầu.

2. Thỏa thuận kết nối chia sẻ dữ liệu

a) Các bộ, cơ quan ngang bộ, cơ quan thuộc chính phủ, Ủy ban nhân dân các tỉnh, thành phố trực thuộc Trung ương xác định và thường xuyên cập nhật các danh mục dữ liệu dùng chung bao gồm cả đặc tả để thực hiện kết nối chia sẻ với Cơ sở dữ liệu tổng hợp quốc gia;

b) Đối với dữ liệu dùng riêng, khi có nhu cầu chia sẻ các bên liên quan phải thiết lập thỏa thuận chia sẻ. Nội dung thỏa thuận chia sẻ bao gồm các bên tham gia; mục đích chia sẻ dữ liệu; phạm vi dữ liệu được chia sẻ; phương thức; thời gian, tần suất chia sẻ.

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 của cơ quan nhà nước có thể thực hiện qua nền tảng điều phối, tích hợp và chia sẻ dữ liệu, cổng dữ liệu, qua tập tin và các phương thức khác tùy theo thỏa thuận chia sẻ giữa các bên.

4. Giám sát hoạt động chia sẻ dữ liệu giữa các cơ quan nhà nước

a) Giám sát chia sẻ dữ liệu của cơ quan nhà nước là điều cần thiết để bảo vệ dữ liệu, bảo đảm chất lượng dữ liệu chia sẻ, cải tiến quy trình thủ tục hành chính và bảo đảm tuân thủ các thỏa thuận chia sẻ;

b) Trung tâm dữ liệu quốc gia thực hiện giám sát hoạt động chia sẻ thông qua hệ thống theo dõi để có đánh giá việc cung cấp và sử dụng dữ liệu được chia sẻ của mỗi cơ quan, đơn vị, xuất bản các báo cáo đánh giá và đề xuất cải tiến;

c) Hệ thống theo dõi đánh giá hoạt động chia sẻ dữ liệu bao gồm các yếu tố về việc công bố và cập nhật kịp thời danh mục dữ liệu dùng chung theo quy định của pháp luật; số lượng nhu cầu chia sẻ dữ liệu; tần suất sử dụng dữ liệu; mức độ hài lòng của người sử dụng dịch vụ mà dữ liệu chia sẻ; số lần sai sót giữa dữ liệu chia sẻ cho cơ sở dữ liệu tổng hợp quốc gia và cơ sở dữ liệu nguồn và các hành vi khác;

d) Khuyến khích các tổ chức cá nhân áp dụng hệ thống theo dõi cho cơ sở dữ liệu của mình.

# Cung cấp dữ liệu cho Cơ sở dữ liệu tổng hợp quốc gia

1. Cơ sở dữ liệu tổng hợp quốc gia có nhu cầu thu thập dữ liệu từ tổ chức, cá nhân để thực hiện phân tích tổng hợp phục vụ công tác chỉ đạo điều hành quốc gia và làm giàu kho dữ liệu mở phục vụ người dân và doanh nghiệp.

2. Tổ chức cá nhân có thể cung cấp dữ liệu tự nguyện dữ liệu cho Trung tâm dữ liệu quốc gia:

a) Tổ chức cá nhân có lưu trữ các dữ liệu quan trọng, hoặc liên quan đến phục vụ công tác phân tích tổng hợp dữ liệu phục vụ chỉ đạo điều hành quốc gia có thể tự nguyện cung cấp dữ liệu cơ sở dữ liệu quốc gia;

b) Trung tâm dữ liệu quốc gia và tổ chức cá nhân ký kết thỏa thuận cung cấp trong đó xác định rõ mục đích cung cấp dữ liệu; phạm vi dữ liệu liệu được cung cấp; phương thức cung cấp dữ liệu; thời gian, tần suất cung cấp và các nội dung liên quan khác;

c) Tổ chức cá nhân cung cấp dữ liệu theo yêu cầu của cơ sở dữ liệu tổng hợp quốc gia để phân tích tổng hợp dữ liệu phục vụ công tác chỉ đạo điều hành quốc gia.

**ĐIỀU KHOẢN THI HÀNH**

# Hiệu lực thi hành

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

# Trách nhiệm của Bộ Công an

1. Chủ trì, phối hợp với Văn phòng Chính phủ, Bộ Thông tin và Truyền thông và bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ, Ủy ban nhân dân cấp tỉnh tổ chức triển khai, hướng dẫn, kiểm tra, đôn đốc việc thực hiện Luật này.

2. Chủ trì, phối hợp với Bộ Thông tin và Truyền thông và cơ quan có liên quan quản lý hoạt động lưu trữ, bảo vệ dữ liệu, bảo đảm an ninh dữ liệu; đấu tranh phòng, chống tội phạm, xử lý vi phạm pháp luật trong hoạt động xử lý, quản trị, điều phối dữ liệu; chủ động phòng ngừa, tham gia đấu tranh với các hành vi vi phạm pháp luật về dữ liệu, hoạt động sử dụng dữ liệu gây phương hại đến an ninh quốc gia, lợi ích của Nhà nước, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân; quản lý, theo dõi, giám sát đối với hoạt động kinh doanh các sản phẩm, dịch vụ về dữ liệu quy định tại khoản 2 Điều 48 Luật 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 Thông tin và Truyền thông 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 Thông tin và Truyền thông 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 Thông tin và Truyền thông, 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.

# Trách nhiệm của Bộ Thông tin và Truyền thông

1. Chủ trì, phối hợp với Bộ Công an, Bộ Quốc phòng, Bộ Khoa học và Công nghệ và cơ quan có liên quan trình Thủ tướng Chính phủ ban hành Chiến lược dữ liệu quốc gia.

2. 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.

3. 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.

# 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.

# Trách nhiệm của Bộ Khoa học và Công nghệ

Phối hợp với Bộ Công an, Bộ Thông tin và Truyền thông 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.

# Trách nhiệm của Bộ Nội vụ

1. Quản lý đối với dữ liệu về công chức, viên chức.

2. Chủ trì, phối hợp với Bộ Thông tin và Truyền thông, 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 đối với dữ liệu về công chức, viên chức.

3. Thực hiện đồng bộ đối với dữ liệu công chức, viên chức về Trung tâm dữ liệu quốc gia theo quy định của Luật này.

# Trách nhiệm của Văn phòng Chính phủ

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.

# 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, Bộ Thông tin và Truyền thông 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.

# 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. Quản lý đối với dữ liệu thuộc phạm vi quản lý theo quy định của pháp luật.

2. Chủ trì, phối hợp với Bộ Thông tin và Truyền thông, 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.

3. Thực hiện đồng bộ dữ liệu thuộc phạm vi quản lý về Trung tâm dữ liệu quốc gia theo quy định của Luật 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; - Ủy ban Giám sát tài chính Quốc gia; - Kiểm toán nhà nước; - Ngân hàng Chính sách xã hội; - Ngân hàng Phát triển Việt Nam; - 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. | **TM. CHÍNH PHỦ**  **THỦ TƯỚNG**  **Phạm Minh Chính** |