QUỐC HỘI	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Luật số: /2026/QH16	*Hà Nội, ngày tháng năm 2026*

LUẬT
AN NINH DỮ LIỆU

Căn cứ Hiến pháp nước Cộng hòa xã hội chủ nghĩa Việt Nam;
Quốc hội ban hành Luật An ninh dữ liệu.

CHƯƠNG I
NHỮNG QUY ĐỊNH CHUNG

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

1. Phạm vi điều chỉnh

Luật này quy định về an ninh dữ liệu; bảo vệ an ninh dữ liệu theo cấp độ rủi ro và vòng đời dữ liệu; quyền, nghĩa vụ, trách nhiệm của cơ quan, tổ chức, cá nhân có liên quan đến bảo vệ an ninh dữ liệu; quản lý nhà nước về an ninh dữ liệu.

2. Đối tượng áp dụng

a) Cơ quan, tổ chức, cá nhân Việt Nam;

b) Cơ quan, tổ chức, cá nhân nước ngoài tại Việt Nam và người gốc Việt Nam chưa xác định được quốc tịch đang sinh sống tại Việt Nam đã được cấp giấy chứng nhận căn cước;

c) Cơ quan, tổ chức, cá nhân nước ngoài trực tiếp tham gia hoặc có liên quan đến hoạt động bảo vệ an ninh dữ liệu và hoạt động xử lý dữ liệu tại Việt Nam.

3. Áp dụng pháp luật

a) Nội dung về bảo vệ dữ liệu cá nhân thực hiện theo Luật Bảo vệ dữ liệu cá nhân; nội dung về an ninh mạng, an ninh hệ thống thông tin thực hiện theo Luật An ninh mạng; nội dung về quản trị, sở hữu, khai thác dữ liệu thực hiện theo Luật Dữ liệu. Luật này không quy định lại các nội dung nêu tại điểm này;

b) Trường hợp Luật này và luật quy định tại điểm a khoản này có quy định khác nhau về biện pháp kỹ thuật, thủ tục bảo đảm an ninh của bản thân dữ liệu thì thực hiện theo quy định của Luật này. Quy định tại điểm này không áp dụng đối với quyền của chủ thể dữ liệu cá nhân (đồng ý, rút lại đồng ý, yêu cầu xóa dữ liệu và quyền khác), thuộc phạm vi điều chỉnh riêng của Luật Bảo vệ dữ liệu cá nhân;

c) Nội dung sửa đổi, bổ sung, bãi bỏ cụ thể đối với từng luật quy định tại điểm a khoản này thực hiện theo Điều 24 của Luật này;

d) Trường hợp pháp luật khác quy định thủ tục hành chính hoặc điều kiện kinh doanh trùng với thủ tục, điều kiện quy định tại Luật này thì thống nhất một thủ tục, một đầu mối tiếp nhận theo quy định của Luật này;

đ) Danh mục dữ liệu quan trọng, dữ liệu cốt lõi thực hiện theo Luật Dữ liệu; cơ chế thử nghiệm có kiểm soát và chứng nhận hợp quy sản phẩm công nghệ số thực hiện theo Luật Chuyển đổi số và Luật Công nghiệp công nghệ số; quản lý rủi ro, thử nghiệm có kiểm soát, gắn nhãn nội dung do trí tuệ nhân tạo tạo ra thực hiện theo Luật Trí tuệ nhân tạo; giá trị pháp lý của thông điệp dữ liệu, chữ ký số thực hiện theo Luật Giao dịch điện tử; căn cứ từ chối tương trợ tư pháp vì lý do chủ quyền, an ninh quốc gia thực hiện theo pháp luật về tương trợ tư pháp;

e) Trường hợp hạ tầng dữ liệu quốc gia trọng yếu đồng thời thuộc Danh mục hệ thống thông tin quan trọng về an ninh quốc gia theo pháp luật về an ninh mạng, việc bảo đảm an ninh mạng của hạ tầng đó thực hiện theo pháp luật về an ninh mạng; việc bảo đảm an ninh của dữ liệu trên hạ tầng đó thực hiện theo Luật này.

Điều 2. Giải thích từ ngữ

Trong Luật này, các từ ngữ dưới đây được hiểu như sau:

1. Dữ liệu là dữ liệu số theo quy định của Luật Dữ liệu.

2. An ninh dữ liệu là sự bảo đảm tính nguyên vẹn, tính bảo mật, tính khả dụng của dữ liệu trong suốt vòng đời; bảo đảm việc xử lý dữ liệu không gây phương hại đến chủ quyền dữ liệu quốc gia, an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân.

3. Bảo vệ an ninh dữ liệu là việc sử dụng lực lượng, phương tiện, biện pháp để phòng ngừa, phát hiện, ngăn chặn, xử lý hành vi xâm phạm an ninh dữ liệu.

4. Vòng đời dữ liệu là toàn bộ quá trình từ khi dữ liệu được tạo lập, thu thập, xử lý theo quy định tại khoản 5 Điều này cho đến khi bị xóa bỏ, tiêu hủy.

5. Xử lý dữ liệu là hoạt động tác động đến dữ liệu theo quy định của Luật Dữ liệu.

6. Cấp độ rủi ro an ninh dữ liệu là mức độ rủi ro an ninh của dữ liệu được xử lý, xác định theo tiêu chí quy định tại Điều 8 của Luật này, làm căn cứ áp dụng biện pháp bảo vệ tương ứng, gồm 04 cấp độ từ thấp đến cao.

7. Chủ quyền dữ liệu quốc gia là quyền quản lý, kiểm soát, bảo vệ của Nhà nước đối với dữ liệu phát sinh trên lãnh thổ Việt Nam hoặc liên quan đến lợi ích quốc gia.

8. Quy mô tích tụ dữ liệu là tổng khối lượng, số lượng chủ thể hoặc mức độ liên kết dữ liệu được thu thập, lưu trữ, xử lý, làm căn cứ xác định sự thay đổi bản chất và cấp độ rủi ro. Xử lý dữ liệu quy mô lớn là hoạt động xử lý dữ liệu đạt ngưỡng do Chính phủ quy định.

9. Ẩn danh hóa là việc xử lý làm cho dữ liệu không còn khả năng xác định trực tiếp hoặc gián tiếp một chủ thể dữ liệu cụ thể và không thể khôi phục ngược lại bằng biện pháp kỹ thuật ở mức chi phí, thời gian hợp lý.

10. Giả danh hóa là việc xử lý sao cho dữ liệu không thể quy về một chủ thể dữ liệu cụ thể nếu không sử dụng thông tin bổ sung được lưu giữ, kiểm soát tách biệt.

11. Tình huống nguy hiểm về an ninh dữ liệu là sự việc, hiện tượng hoặc hành vi đe dọa xâm phạm an ninh dữ liệu.

12. Hạ tầng dữ liệu quốc gia trọng yếu là trung tâm dữ liệu, cơ sở dữ liệu quốc gia, cơ sở dữ liệu chuyên ngành trọng điểm và hạ tầng mạng phục vụ dữ liệu Cấp độ 4, dữ liệu Cấp độ 3 có ý nghĩa chiến lược mà sự cố sẽ ảnh hưởng nghiêm trọng đến lĩnh vực thiết yếu của đời sống xã hội, quốc phòng, an ninh quốc gia.

13. An ninh hạ tầng dữ liệu xanh và bền vững là việc bảo đảm sự sẵn sàng, liên tục và an toàn của hạ tầng lưu trữ, xử lý dữ liệu thông qua các giải pháp nâng cao hiệu quả sử dụng năng lượng, năng lượng tái tạo, tối ưu hóa tài nguyên làm mát và khả năng chống chịu trước các sự cố lưới điện, thảm họa thiên nhiên và biến đổi khí hậu.

14. Trung tâm Quản trị an ninh dữ liệu quốc gia là đơn vị thuộc lực lượng chuyên trách bảo vệ an ninh mạng Bộ Công an, thực hiện giám sát, điều phối ứng cứu sự cố và quản trị rủi ro an ninh dữ liệu.

15. Mật mã kháng lượng tử là giải pháp mật mã có khả năng chống lại phương thức phân tích, giải mã sử dụng điện toán lượng tử, đã được cơ quan có thẩm quyền thẩm định, chứng nhận.

16. Mật mã an ninh là giải pháp mật mã do cơ quan chuyên trách về bảo vệ an ninh mạng thuộc Bộ Công an nghiên cứu, phát triển, kiểm định, công bố, phục vụ bảo đảm an ninh mạng, an ninh dữ liệu.

17. Biện pháp cưỡng chế kỹ thuật là biện pháp kỹ thuật do cấp có thẩm quyền quyết định áp dụng đối với tổ chức, cá nhân vi phạm, gồm giới hạn băng thông, tạm ngừng hoặc đình chỉ quyền truy cập, ngăn chặn luồng dữ liệu, bảo đảm không gây gián đoạn dịch vụ đối với người dùng không liên quan đến hành vi vi phạm; không bao gồm biện pháp thu hồi giấy phép.

18. Dữ liệu độc hại là dữ liệu có nội dung xâm phạm an ninh quốc gia, trật tự, an toàn xã hội hoặc chứa mã độc, dữ liệu bị đầu độc nhằm phá hoại, làm sai lệch hoạt động của hệ thống thông tin, mô hình trí tuệ nhân tạo.

19. Hệ thống giám sát an ninh dữ liệu tập trung quốc gia là hệ thống kỹ thuật do Trung tâm Quản trị an ninh dữ liệu quốc gia quản lý, vận hành, thực hiện tiếp nhận, phân tích siêu dữ liệu an ninh, nhật ký sự kiện phục vụ giám sát, cảnh báo sớm rủi ro an ninh dữ liệu theo quy định tại Điều 18 của Luật này.

20. Đầu độc dữ liệu là hành vi cố ý chèn, sửa đổi hoặc làm sai lệch dữ liệu huấn luyện, luồng dữ liệu đầu vào nhằm làm biến dạng chức năng, tạo lỗ hổng ẩn hoặc làm sai lệch kết quả xử lý của hệ thống thông tin, mô hình trí tuệ nhân tạo.

21. Bên xử lý dữ liệu là tổ chức, cá nhân được chủ sở hữu dữ liệu hoặc chủ quản dữ liệu ủy quyền, giao kết hợp đồng để thực hiện một hoặc một số hoạt động xử lý dữ liệu quy định tại khoản 5 Điều này. Trường hợp dữ liệu được xử lý là dữ liệu cá nhân, việc xác định bên xử lý dữ liệu thực hiện theo quy định của pháp luật về bảo vệ dữ liệu cá nhân.

22. Đánh giá tác động an ninh dữ liệu là việc phân tích ảnh hưởng của hoạt động xử lý dữ liệu đối với an ninh quốc gia, lợi ích công cộng và an ninh của hệ thống dữ liệu, thực hiện theo quy định tại Điều 10 của Luật này.

23. Hợp đồng an ninh dữ liệu là hợp đồng hoặc điều khoản trong hợp đồng dịch vụ quy định quyền, nghĩa vụ bảo vệ an ninh dữ liệu giữa các bên khi chia sẻ, chuyển giao hoặc cho phép bên thứ ba tiếp cận dữ liệu theo quy định tại Điều 16 của Luật này.

Điều 3. Nguyên tắc bảo vệ an ninh dữ liệu

1. Tuân thủ Hiến pháp, pháp luật; bảo đảm an ninh quốc gia, lợi ích công cộng, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân.

2. Đặt dưới sự lãnh đạo của Đảng Cộng sản Việt Nam, sự quản lý thống nhất của Nhà nước; phát huy vai trò nòng cốt của lực lượng chuyên trách bảo vệ an ninh dữ liệu và sức mạnh tổng hợp của cơ quan, tổ chức, cá nhân có liên quan.

3. Kết hợp chặt chẽ giữa bảo vệ an ninh dữ liệu với thúc đẩy phát triển kinh tế số, xã hội số; bảo đảm quyền con người, quyền công dân.

4. Bảo vệ an ninh dữ liệu phải dựa trên đánh giá và quản lý rủi ro theo từng cấp độ; được thực hiện chủ động từ giai đoạn thiết kế, thiết lập mặc định và xuyên suốt toàn bộ vòng đời của dữ liệu.

5. Áp dụng các biện pháp để bảo vệ chủ quyền dữ liệu quốc gia; chủ động phòng ngừa, phát hiện, ngăn chặn, đấu tranh làm thất bại mọi hoạt động xâm

phạm an ninh dữ liệu; xử lý kịp thời, nghiêm minh các hành vi vi phạm pháp luật về an ninh dữ liệu.

6. Thực hiện đồng bộ các biện pháp bảo vệ an ninh dữ liệu với các biện pháp bảo vệ an ninh mạng, bảo vệ dữ liệu cá nhân theo quy định của pháp luật.

7. Khuyến khích, bảo đảm sự lưu thông dữ liệu hợp pháp, an toàn và thông suốt; phát huy nội lực kết hợp với đẩy mạnh hợp tác quốc tế, áp dụng có chọn lọc các tiêu chuẩn, chuẩn mực quốc tế về an ninh dữ liệu.

8. Việc thẩm định, đánh giá, chứng nhận về an ninh dữ liệu quy định tại Luật này được thực hiện trên nguyên tắc tích hợp, kế thừa kết quả đã có, không tổ chức nhiều lần cho cùng một đối tượng, cùng một nội dung.

Điều 4. Chính sách của Nhà nước về an ninh dữ liệu

1. Nhà nước ưu tiên hoàn thiện thể chế, chính sách về an ninh dữ liệu; xây dựng hệ thống tài nguyên dữ liệu quốc gia an toàn, tin cậy; bảo vệ và xác lập chủ quyền dữ liệu quốc gia.

2. Bảo đảm an ninh dữ liệu gắn liền với đẩy mạnh đầu tư, phát triển hạ tầng dữ liệu quốc gia trọng yếu, hạ tầng xử lý dữ liệu quy mô lớn và tốc độ cao, hạ tầng dữ liệu xanh và tiết kiệm năng lượng; hỗ trợ nâng cao năng lực tự chủ, tính chống chịu và an toàn cho các hạ tầng dữ liệu, trung tâm dữ liệu.

3. Khuyến khích, tạo điều kiện thuận lợi cho tổ chức, cá nhân nghiên cứu, phát triển, ứng dụng trí tuệ nhân tạo và công nghệ mới trong bảo vệ an ninh dữ liệu; thúc đẩy đổi mới sáng tạo và phát triển kinh tế dữ liệu an toàn, bền vững.

4. Chú trọng đào tạo, thu hút và phát triển nguồn nhân lực chất lượng cao về an ninh dữ liệu; mở rộng và nâng cao hiệu quả hợp tác quốc tế, tiếp thu công nghệ tiên tiến và chủ động tham gia các cơ chế bảo đảm an ninh dữ liệu khu vực và toàn cầu.

5. Bảo đảm ngân sách nhà nước cho hoạt động bảo vệ an ninh dữ liệu; khuyến khích, huy động các nguồn lực xã hội hóa hợp pháp để đầu tư, phát triển công nghệ và dịch vụ an ninh dữ liệu.

6. Chính phủ cụ thể hóa chính sách của Nhà nước về an ninh dữ liệu trong từng thời kỳ phù hợp với chiến lược phát triển kinh tế - xã hội và bảo đảm an ninh quốc gia.

Điều 5. Các hành vi bị nghiêm cấm

1. Xử lý dữ liệu trái phép, bao gồm chiếm đoạt, mua bán, làm lộ dữ liệu; ngăn chặn truy cập trái phép dữ liệu.

2. Sử dụng dữ liệu hoặc làm giả dữ liệu nhằm xâm phạm an ninh quốc gia, trật tự, an toàn xã hội.

3. Lợi dụng hoặc lạm dụng hoạt động hoặc quyền hạn được giao trong bảo vệ an ninh dữ liệu để xâm phạm chủ quyền dữ liệu quốc gia, lợi ích quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân hoặc để trục lợi.

4. Che giấu, không thông báo hoặc báo cáo sai sự thật về sự cố an ninh dữ liệu; chống lại hoặc cản trở hoạt động của lực lượng bảo vệ an ninh dữ liệu, hoạt động thanh tra, kiểm tra, điều tra của cơ quan có thẩm quyền; tấn công, vô hiệu hóa trái pháp luật biện pháp bảo vệ an ninh dữ liệu.

5. Cố ý tách nhỏ, chia phần hoặc khai báo sai cấp độ rủi ro an ninh dữ liệu nhằm né tránh nghĩa vụ bảo vệ tương ứng.

6. Hành vi khác xâm phạm an ninh dữ liệu theo quy định của pháp luật.

Điều 6. Các biện pháp bảo vệ an ninh dữ liệu

1. Các biện pháp bảo vệ an ninh dữ liệu bao gồm:

a) Biện pháp quản lý, bao gồm: phân loại và xác định cấp độ rủi ro an ninh dữ liệu và áp dụng biện pháp bảo vệ tương ứng; ban hành chính sách, quy trình, nội quy bảo vệ an ninh dữ liệu; phân công, bố trí nhân sự, bộ phận chuyên trách an ninh dữ liệu; quản lý truy cập, định danh, phân quyền; tổ chức tuyên truyền, đào tạo, diễn tập;

b) Biện pháp kỹ thuật bảo vệ theo vòng đời dữ liệu, bao gồm: áp dụng giải pháp an ninh từ giai đoạn thiết kế và theo mặc định; sử dụng mật mã cơ yếu, mật mã an ninh, mật mã dân sự theo quy định của pháp luật, áp dụng tiêu chuẩn kỹ thuật kháng lượng tử theo lộ trình quy định tại Điều 15 của Luật này đối với dữ liệu Cấp độ 4, dữ liệu Cấp độ 3 có ý nghĩa chiến lược quốc gia; sao lưu, dự phòng, phục hồi dữ liệu; bảo vệ an toàn hạ tầng vật lý, thiết bị lưu trữ, môi trường xử lý dữ liệu và thiết bị đầu cuối; tiêu hủy dữ liệu an toàn;

c) Biện pháp giám sát, cảnh báo sớm và kiểm toán, bao gồm: giám sát an ninh dữ liệu tập trung, liên tục; cảnh báo sớm nguy cơ, rủi ro và lỗ hổng an ninh dữ liệu; kiểm toán an ninh dữ liệu định kỳ; kiểm tra, giám sát việc tuân thủ pháp luật về an ninh dữ liệu;

d) Biện pháp đánh giá, thẩm định và chứng nhận, bao gồm: thẩm định an ninh dữ liệu đối với dự án đầu tư, hệ thống thông tin, ứng dụng công nghệ mới và hoạt động chuyển giao công nghệ; đánh giá rủi ro; kiểm thử an ninh dữ liệu; đánh giá rủi ro trong luân chuyển, cung cấp dữ liệu xuyên biên giới; đánh giá, chứng nhận hợp quy sản phẩm, dịch vụ an ninh dữ liệu;

đ) Biện pháp ứng phó, khắc phục sự cố, bao gồm: xây dựng, ban hành kịch bản ứng phó sự cố; kích hoạt quy trình ứng phó, khắc phục, diễn tập và điều tra nguyên nhân sự cố an ninh dữ liệu;

e) Biện pháp khẩn cấp và xử lý đặc biệt, bao gồm: tạm dừng, ngăn chặn, vô hiệu hóa việc xử lý, luân chuyển dữ liệu; yêu cầu gỡ bỏ, xóa bỏ dữ liệu có nội dung vi phạm pháp luật hoặc đe dọa trực tiếp đến an ninh quốc gia; áp dụng các biện pháp cưỡng chế kỹ thuật để ứng cứu sự cố an ninh dữ liệu đặc biệt nghiêm trọng.

2. Chủ quản dữ liệu có trách nhiệm trực tiếp áp dụng các biện pháp bảo vệ an ninh dữ liệu quy định tại khoản 1 Điều này trong phạm vi được giao xây dựng, quản lý, vận hành, khai thác dữ liệu và chịu trách nhiệm trước chủ sở hữu dữ liệu, trước pháp luật về việc thực hiện các biện pháp đó; trường hợp có thiệt hại xảy ra do lỗi của nhiều chủ thể thì áp dụng nguyên tắc trách nhiệm liên đới theo quy định của Bộ luật Dân sự. Chủ sở hữu dữ liệu chịu trách nhiệm cuối cùng về an ninh đối với dữ liệu thuộc quyền sở hữu.

3. Việc áp dụng các biện pháp bảo vệ an ninh dữ liệu phải phù hợp với cấp độ rủi ro an ninh dữ liệu theo Điều 8 của Luật này và diễn biến mức độ rủi ro thực tế; bảo đảm tính cần thiết, tương xứng, hiệu quả và hạn chế tối đa tác động tiêu cực đến hoạt động hợp pháp của chủ thể dữ liệu; các biện pháp cưỡng chế kỹ thuật hoặc hạn chế quyền phải được chấm dứt ngay khi căn cứ áp dụng không còn.

4. Cụ thể hóa điểm b khoản 1 Điều này: Mật mã an ninh quy định tại khoản 16 Điều 2 của Luật này được cơ quan, tổ chức, cá nhân lựa chọn áp dụng trong các biện pháp bảo vệ an ninh dữ liệu theo Luật này; không áp dụng để bảo vệ dữ liệu bí mật nhà nước. Việc bảo vệ dữ liệu bí mật nhà nước bằng kỹ thuật mật mã thực hiện thống nhất theo pháp luật về cơ yếu. Chính phủ quy định chi tiết điều kiện công bố, kiểm định giải pháp mật mã an ninh quy định tại khoản này.

5. Chính phủ quy định chi tiết thẩm quyền, trình tự, thủ tục áp dụng các biện pháp quy định tại khoản 1 Điều này, trong đó bao gồm tối thiểu các nội dung sau đây: mức xác thực và kiểm soát truy cập tối thiểu đối với hệ thống thông tin xử lý dữ liệu Cấp độ 3, dữ liệu Cấp độ 4; thời hạn lưu trữ nhật ký truy cập, nhật ký xử lý dữ liệu; tần suất sao lưu và kiểm tra định kỳ khả năng phục hồi dữ liệu; tần suất, nội dung đào tạo, nâng cao nhận thức an ninh dữ liệu cho người lao động; tiêu chuẩn năng lực và điều kiện bảo đảm tính độc lập của nhân sự an ninh dữ liệu chuyên trách quy định tại điểm a khoản 1 Điều này và nhân sự phụ trách an ninh dữ liệu quy định tại điểm b khoản 3 Điều 8 của Luật này.

Điều 7. Hợp tác quốc tế về an ninh dữ liệu

1. Hợp tác quốc tế về an ninh dữ liệu thực hiện trên nguyên tắc tôn trọng độc lập, chủ quyền, bình đẳng, cùng có lợi, phù hợp với Hiến pháp, pháp luật Việt Nam và điều ước quốc tế mà nước Cộng hòa xã hội chủ nghĩa Việt Nam là thành viên.

2. Nội dung hợp tác quốc tế về an ninh dữ liệu bao gồm: ký kết, thực thi điều ước, thỏa thuận quốc tế; phối hợp kỹ thuật, thu thập, chia sẻ dữ liệu điện tử phục vụ phòng, chống tội phạm; dẫn độ, chuyển giao người phạm tội; phong tỏa, thu hồi tài sản số; ứng cứu sự cố an ninh dữ liệu xuyên biên giới; công nhận, thi hành phán quyết của tòa án nước ngoài trên cơ sở có đi có lại.

3. Bộ Công an là cơ quan đầu mối tham mưu, đề xuất chủ trương đàm phán, ký kết điều ước quốc tế về an ninh dữ liệu và phòng, chống tội phạm về dữ liệu theo quy định của pháp luật về điều ước quốc tế; phối hợp với tổ chức thực thi pháp luật quốc tế và doanh nghiệp công nghệ xuyên quốc gia để truy vết, ứng cứu sự cố; thiết lập nền tảng chia sẻ thông tin an ninh dữ liệu quốc gia trên cơ sở tự nguyện, bảo đảm ẩn danh và miễn trừ trách nhiệm cho bên chia sẻ có thiện chí.

4. Chính phủ quy định chi tiết cơ chế vận hành nền tảng chia sẻ thông tin và cơ chế phối hợp ứng cứu sự cố an ninh dữ liệu xuyên biên giới quy định tại Điều này.

CHƯƠNG II
BẢO VỆ AN NINH DỮ LIỆU THEO CẤP ĐỘ RỦI RO VÀ VÒNG ĐỜI DỮ LIỆU

Điều 8. Cấp độ rủi ro an ninh dữ liệu

1. Cấp độ rủi ro an ninh dữ liệu là mức độ rủi ro an ninh của dữ liệu được xử lý, xác định trên cơ sở đánh giá rủi ro theo tiêu chí quy định tại khoản 2 Điều này, gồm 04 cấp độ từ thấp đến cao:

a) Cấp độ 1: dữ liệu được phép tiếp cận công khai hoặc không giới hạn đối tượng truy cập; nếu bị xâm phạm chỉ gây rủi ro thấp, không gây thiệt hại đáng kể;

b) Cấp độ 2: dữ liệu lưu hành trong phạm vi nội bộ cơ quan, tổ chức, doanh nghiệp hoặc là bí mật kinh doanh; nếu bị rò rỉ gây tổn thất cho hoạt động, uy tín của tổ chức nhưng chưa gây nguy hại cho an ninh quốc gia, trật tự, an toàn xã hội hoặc lợi ích công cộng;

c) Cấp độ 3: dữ liệu thuộc Danh mục dữ liệu quan trọng do Thủ tướng Chính phủ ban hành theo Luật Dữ liệu;

d) Cấp độ 4: dữ liệu thuộc Danh mục dữ liệu cốt lõi do Thủ tướng Chính phủ ban hành theo Luật Dữ liệu.

2. Việc xác định cấp độ rủi ro quy định tại khoản 1 Điều này căn cứ vào: khả năng dữ liệu bị truy cập, khai thác, sử dụng trái phép hoặc bị tấn công mạng; mức độ nhạy cảm của dữ liệu, có xét đến kết quả phân loại dữ liệu theo Luật Dữ liệu; quy mô, phạm vi ảnh hưởng nếu dữ liệu bị lộ, mất, sửa đổi hoặc phá hủy

trái phép; mức độ liên quan đến quốc phòng, an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân.

3. Nguyên tắc bảo vệ theo cấp độ rủi ro:

a) Dữ liệu Cấp độ 1, Cấp độ 2: chủ quản dữ liệu tự xác định cấp độ, tự tổ chức bảo vệ theo tiêu chuẩn, quy chuẩn kỹ thuật hiện hành và tự chịu trách nhiệm, không phải báo cáo hoặc xin xác nhận của cơ quan nhà nước;

b) Dữ liệu Cấp độ 3, Cấp độ 4: chủ quản dữ liệu phải thiết lập cơ chế quản trị rủi ro, bố trí nhân sự phụ trách an ninh dữ liệu và áp dụng biện pháp bảo vệ quy định tại Điều 6 của Luật này, theo quy định của Chính phủ;

c) Doanh nghiệp nhỏ, doanh nghiệp siêu nhỏ và doanh nghiệp khởi nghiệp sáng tạo không xử lý dữ liệu quy mô lớn, không xử lý dữ liệu Cấp độ 3, Cấp độ 4 được miễn thực hiện nghĩa vụ quy định tại điểm b khoản này.

4. Hệ thống thông tin xử lý dữ liệu phải đáp ứng yêu cầu an ninh tương ứng với cấp độ rủi ro cao nhất của dữ liệu được xử lý; trường hợp áp dụng phân vùng hoặc cách ly dữ liệu, yêu cầu an ninh được áp dụng theo cấp độ rủi ro của từng phân vùng. Đối với dữ liệu Cấp độ 4 thuộc lĩnh vực quân sự, quốc phòng, an ninh, đối ngoại hoặc chứa bí mật nhà nước, bắt buộc áp dụng biện pháp cách ly vật lý; đối với dữ liệu Cấp độ 4 thuộc lĩnh vực khác, được áp dụng biện pháp phân vùng logic nghiêm ngặt đáp ứng tiêu chuẩn kỹ thuật tương đương cách ly vật lý, không bắt buộc cách ly vật lý; tiêu chuẩn kỹ thuật cụ thể thực hiện theo quy định của Chính phủ tại khoản 8 Điều này. Tiêu chuẩn kỹ thuật cách ly vật lý đối với dữ liệu chứa bí mật nhà nước bằng kỹ thuật mật mã cơ yếu do Ban Cơ yếu Chính phủ chủ trì, phối hợp Bộ Công an quy định.

5. Việc tích tụ dữ liệu đạt ngưỡng quy mô lớn hoặc có thay đổi cơ bản về mục đích, phạm vi xử lý dữ liệu làm phát sinh yêu cầu bảo vệ tương ứng mức độ rủi ro thực tế, nhưng không tự động làm thay đổi cấp độ pháp lý của dữ liệu. Dữ liệu Cấp độ 3, Cấp độ 4 được xác định duy nhất theo Danh mục dữ liệu quan trọng, dữ liệu cốt lõi do Thủ tướng Chính phủ ban hành theo Luật Dữ liệu; việc tích tụ hoặc thay đổi hoạt động xử lý không tự động chuyển dữ liệu Cấp độ 1, Cấp độ 2 sang Cấp độ 3, Cấp độ 4 nếu dữ liệu chưa được cập nhật vào Danh mục nêu trên. Chủ quản dữ liệu có trách nhiệm áp dụng ngay biện pháp bảo vệ tương xứng mức độ rủi ro thực tế khi quy mô tích tụ đạt ngưỡng quy mô lớn, đồng thời đăng ký biến động quy mô tích tụ theo thủ tục một cửa quy định tại Điều 20 của Luật này. Đối với hệ thống thông tin mới xây dựng, chưa có đủ dữ liệu để đánh giá quy mô tích tụ, chủ quản hệ thống thực hiện đánh giá lại định kỳ theo hướng dẫn của Chính phủ, không bắt buộc đánh giá tại thời điểm chưa phát sinh dữ liệu.

6. Việc xác định dữ liệu Cấp độ 1, Cấp độ 2 quy định tại điểm a, điểm b khoản 1 Điều này được thực hiện như sau:

a) Đối với cơ quan nhà nước: trước hết xác định dữ liệu thuộc Danh mục dữ liệu quan trọng hay Danh mục dữ liệu cốt lõi theo Luật Dữ liệu; dữ liệu thuộc Danh mục dữ liệu quan trọng được xác định Cấp độ 3, dữ liệu thuộc Danh mục dữ liệu cốt lõi được xác định Cấp độ 4 theo quy định tại khoản 1 Điều này. Đối với dữ liệu không thuộc hai Danh mục nêu trên, cấp độ rủi ro được xác định trên cơ sở kết quả phân loại dữ liệu theo tính chất chia sẻ quy định tại điểm a khoản 1 Điều 13 của Luật Dữ liệu: dữ liệu mở tương ứng Cấp độ 1; dữ liệu dùng riêng, dữ liệu dùng chung tương ứng Cấp độ 2, trừ trường hợp phạm vi đối tượng được chia sẻ, tiếp cận rộng và mức độ nhạy cảm thấp theo tiêu chí quy định tại khoản 2 Điều này thì tương ứng Cấp độ 1;

b) Đối với tổ chức, cá nhân ngoài khu vực nhà nước: chủ quản dữ liệu tự xác định cấp độ trên cơ sở tiêu chí định tính quy định tại khoản 2 Điều này và Bảng tự đánh giá cấp độ rủi ro an ninh dữ liệu do Bộ Công an ban hành, tự chịu trách nhiệm về kết quả tự xác định;

c) Đối với cơ quan Đảng, Ủy ban Mặt trận Tổ quốc Việt Nam, tổ chức chính trị - xã hội: việc xác định cấp độ rủi ro thực hiện theo nguyên tắc tự quản dữ liệu quy định tại Điều 9 của Luật Dữ liệu, do cơ quan có thẩm quyền của cơ quan, tổ chức đó quyết định, tự chịu trách nhiệm về kết quả xác định.

7. Tiêu chí, danh mục xác định dữ liệu Cấp độ 3, Cấp độ 4 thực hiện theo quy định về Danh mục dữ liệu quan trọng, dữ liệu cốt lõi của Luật Dữ liệu; thủ tục đánh giá, xác nhận cấp độ được tích hợp trong quy trình thẩm định an ninh mạng hoặc hậu kiểm.

8. Chính phủ quy định chi tiết Điều này, bao gồm: biện pháp bảo vệ tương ứng với từng cấp độ rủi ro quy định tại khoản 3 Điều này; phương án phân vùng logic, cách ly vật lý, xử lý hỗn hợp và cơ chế liên thông với cấp độ an toàn hệ thống thông tin theo pháp luật về an ninh mạng quy định tại khoản 4 Điều này; thời hạn hoàn thành nâng cấp biện pháp bảo vệ khi phát sinh yêu cầu bảo vệ tương xứng mức độ rủi ro thực tế quy định tại khoản 5 Điều này.

9. Việc xác định quy mô tích tụ dữ liệu để tính cấp độ rủi ro và áp dụng nghĩa vụ tương ứng theo Luật này được tính trên tổng khối lượng dữ liệu do doanh nghiệp trực tiếp xử lý trên lãnh thổ Việt Nam; trường hợp doanh nghiệp và chi nhánh, công ty con, đơn vị phụ thuộc cùng khai thác, kết hợp hoặc có khả năng kiểm soát chung một tập dữ liệu thì được tính gộp quy mô tích tụ của các đơn vị đó. Công ty con là pháp nhân độc lập, không cùng khai thác hoặc kết hợp dữ liệu với công ty mẹ thì không bị tính gộp quy mô tích tụ theo khoản này.

Điều 9. Bảo vệ an ninh dữ liệu theo vòng đời dữ liệu

1. Trong giai đoạn thu thập, khởi tạo và thiết kế hệ thống: tổ chức, cá nhân phát triển, sản xuất, cung cấp, sử dụng hệ thống, thiết bị, phần mềm để thu thập, khởi tạo dữ liệu phải tích hợp biện pháp an ninh ngay từ thiết kế và trong suốt vòng đời sản phẩm; chỉ thu thập đúng, đủ thông tin thực sự cần thiết cho mục đích đã tuyên bố. Nhân sự tiếp cận hệ thống xử lý dữ liệu Cấp độ 4 phải được sàng lọc, cam kết bảo mật và phân quyền truy cập tối thiểu.

2. Trong giai đoạn lưu trữ (dữ liệu tĩnh): dữ liệu từ Cấp độ 3 lưu trữ tại trung tâm dữ liệu hoặc qua bên thứ ba phải đáp ứng tiêu chuẩn an ninh vật lý, an ninh mạng, an ninh nguồn điện dự phòng, hiệu quả sử dụng năng lượng, giải pháp làm mát an toàn môi trường, quản lý khóa mật mã và cơ chế sao lưu, phục hồi khẩn cấp. Dữ liệu Cấp độ 3, dữ liệu Cấp độ 4 có giá trị lưu trữ lâu dài phải lưu ít nhất một bản gốc tách biệt vật lý hoặc logic với bản sao lưu vận hành. Các trung tâm dữ liệu lưu trữ dữ liệu Cấp độ 4, dữ liệu Cấp độ 3 phải có phương án bảo đảm vận hành liên tục trước sự cố gián đoạn nguồn điện lưới quốc gia và thảm họa môi trường.

3. Trong giai đoạn truyền dẫn, xử lý (dữ liệu động): dữ liệu từ Cấp độ 3 khi truyền dẫn phải được mã hóa, xác thực; luồng dữ liệu Cấp độ 4 giữa cơ quan nhà nước và hạ tầng trọng yếu phải qua kênh chuyên biệt, kiểm soát phiên truy cập và giám sát liên tục. Hoạt động xử lý phải đúng mục đích đã xác định và thực hiện đánh giá tác động an ninh dữ liệu theo Điều 10 của Luật này khi thuộc trường hợp phải đánh giá. Quản lý khóa mật mã bảo vệ dữ liệu Cấp độ 3, dữ liệu Cấp độ 4 thực hiện theo tiêu chuẩn do Bộ Công an trình cấp có thẩm quyền ban hành, đối với dữ liệu có chứa bí mật nhà nước do Ban Cơ yếu Chính phủ chủ trì, phối hợp với Bộ Công an trình cấp có thẩm quyền ban hành; nghiêm cấm tiết lộ khóa mật mã cho tổ chức, cá nhân không có thẩm quyền.

4. Trong giai đoạn chia sẻ, cung cấp, giao dịch: việc chia sẻ, cung cấp dữ liệu phải có cơ sở pháp lý và áp dụng biện pháp bảo vệ tương ứng cấp độ dữ liệu; nghiêm cấm chia sẻ dữ liệu của cơ quan nhà nước nếu có nguy cơ gây phương hại an ninh quốc gia. Việc kinh doanh, chuyển nhượng dữ liệu thực hiện theo pháp luật về dữ liệu; trường hợp chuyển nhượng, chuyển giao dữ liệu ra nước ngoài thực hiện theo Điều 17 của Luật này.

5. Trong giai đoạn tiêu hủy: chủ quản dữ liệu có trách nhiệm định kỳ rà soát, phân loại dữ liệu không còn giá trị sử dụng để quyết định tiêu hủy hoặc tái cấu trúc, tiếp tục lưu trữ phù hợp mục đích mới; tần suất, tiêu chí xác định dữ liệu không còn giá trị sử dụng do chủ quản dữ liệu tự quyết định phù hợp đặc thù lĩnh vực, quy mô hoạt động, trừ trường hợp pháp luật chuyên ngành có quy định khác. Khi hết thời hạn lưu trữ hoặc không còn mục đích xử lý hợp pháp, chủ quản dữ liệu phải tiêu hủy dữ liệu, trừ trường hợp pháp luật có quy định

khác; dữ liệu từ Cấp độ 3 phải được tiêu hủy triệt để bằng biện pháp kỹ thuật chuyên dụng, bảo đảm không thể khôi phục. Đối với dữ liệu đã được mã hóa toàn phần lưu trữ trên hạ tầng đám mây, hệ thống sao lưu đa tầng hoặc lưu trữ phân tán mà không thể xóa vật lý triệt để, được áp dụng biện pháp hủy khóa mã hóa làm cho dữ liệu không thể đọc, khôi phục. Chủ quản dữ liệu lập và lưu hồ sơ tiêu hủy để cung cấp cho cơ quan chức năng khi có yêu cầu.

6. Chính phủ quy định chi tiết tiêu chuẩn kỹ thuật an ninh theo thiết kế, tiêu chuẩn lưu trữ, truyền dẫn, mã hóa và tiêu chuẩn, phương pháp tiêu hủy dữ liệu an toàn quy định tại Điều này.

Điều 10. Kiểm kê, đánh giá tác động, kiểm toán và chứng nhận an ninh dữ liệu

1. Chủ quản dữ liệu có trách nhiệm thiết lập, duy trì, cải tiến phương án bảo vệ an ninh dữ liệu phù hợp quy mô hoạt động, tính chất dữ liệu và mức độ rủi ro; kiểm kê dữ liệu thường xuyên; lập bản đồ dữ liệu đối với dữ liệu Cấp độ 3, dữ liệu Cấp độ 4.

2. Chủ quản hệ thống thông tin xử lý dữ liệu Cấp độ 4, dữ liệu Cấp độ 3 có trách nhiệm tự tổ chức đánh giá rủi ro, kiểm toán an ninh dữ liệu định kỳ hằng năm và báo cáo Bộ Công an; thực hiện đánh giá, kiểm toán đột xuất khi đưa hệ thống mới vào vận hành, khi thay đổi làm tăng cấp độ rủi ro an ninh dữ liệu, sau khi xảy ra sự cố nghiêm trọng hoặc theo yêu cầu của cơ quan có thẩm quyền.

3. Đánh giá tác động an ninh dữ liệu quy định tại khoản 22 Điều 2 của Luật này phải được thực hiện trước khi triển khai hệ thống mới, xử lý dữ liệu Cấp độ 3, dữ liệu Cấp độ 4, thay đổi kiến trúc hệ thống, chuyển dữ liệu ra ngoài phạm vi quản lý hoặc sử dụng công nghệ mới có nguy cơ ảnh hưởng an ninh dữ liệu. Trường hợp dữ liệu đồng thời là dữ liệu cá nhân, hồ sơ đánh giá tác động an ninh dữ liệu được tích hợp với hồ sơ đánh giá tác động xử lý dữ liệu cá nhân, không lập hai bộ hồ sơ riêng biệt.

4. Tự đánh giá rủi ro, kiểm toán, thẩm định an ninh dữ liệu, chứng nhận hợp quy và đánh giá tác động an ninh dữ liệu của Luật này có bản chất và giá trị pháp lý khác nhau nhưng được tổ chức thực hiện thống nhất theo thủ tục hành chính quy định tại Luật này.

5. Sản phẩm, dịch vụ công nghệ thông tin chuyên dùng phục vụ bảo vệ, mã hóa, giám sát an ninh dữ liệu phải được chứng nhận hợp quy trước khi lưu thông; sản phẩm đã có chứng chỉ bảo mật quốc tế uy tín được công nhận tương đương. Sản phẩm, dịch vụ đã được chứng nhận hợp quy về an ninh mạng theo pháp luật về an ninh mạng đối với chức năng bảo vệ an ninh dữ liệu tương ứng thì không phải thực hiện lại thủ tục chứng nhận hợp quy về an ninh dữ liệu đối với chức năng đó. Đối với sản phẩm, dịch vụ phục vụ trực tiếp hệ thống xử lý dữ

liệu Cấp độ 4 của cơ quan Đảng, Nhà nước, lực lượng vũ trang thì Bộ Công an chủ trì thực hiện kiểm định an ninh chuyên biệt trước khi sử dụng.

6. Chủ quản dữ liệu tự chịu trách nhiệm về tính chính xác của việc tự xác định cấp độ, tự chứng nhận tuân thủ đối với dữ liệu Cấp độ 1, dữ liệu Cấp độ 2; chấp hành nghĩa vụ thẩm định, kiểm toán và kết nối, chia sẻ thông tin giám sát với Hệ thống giám sát an ninh dữ liệu tập trung quốc gia đối với dữ liệu Cấp độ 3, dữ liệu Cấp độ 4.

7. Chính phủ quy định chi tiết tần suất, nội dung, hồ sơ, điều kiện, trình tự đánh giá rủi ro, kiểm toán, chứng nhận an ninh dữ liệu và tỷ lệ hậu kiểm.

8. Việc xác định, quản lý rủi ro theo Điều 25 Luật Dữ liệu được thực hiện thống nhất theo tiêu chí, quy trình xác định cấp độ rủi ro an ninh dữ liệu quy định tại Điều 8 của Luật này, không tổ chức đánh giá hai lần theo hai bộ tiêu chí khác nhau cho cùng một đối tượng.

CHƯƠNG III
BẢO VỆ AN NINH DỮ LIỆU TRONG XỬ LÝ DỮ LIỆU QUY MÔ LỚN, KINH TẾ SỐ, CHÍNH PHỦ SỐ, HẠ TẦNG SỐ VÀ LƯU CHUYỂN DỮ LIỆU XUYÊN BIÊN GIỚI

Điều 11. Xử lý dữ liệu quy mô lớn và phối hợp áp dụng biện pháp an ninh mạng, an ninh dữ liệu

1. Khi triển khai các biện pháp bảo vệ an ninh mạng có tác động đến dữ liệu, cơ quan, tổ chức, cá nhân thực hiện phải đồng thời bảo đảm tính bảo mật, nguyên vẹn, khả dụng của dữ liệu; không làm lộ, mất, sai lệch hoặc phá hủy trái phép dữ liệu Cấp độ 3, dữ liệu Cấp độ 4.

2. Hoạt động xử lý dữ liệu quy mô lớn phải thực hiện đánh giá tác động an ninh dữ liệu theo Điều 10 của Luật này; đối với dữ liệu có khả năng nhận diện hoặc tái nhận diện chủ thể, phải ẩn danh hóa hoặc giả danh hóa trước khi kết hợp dữ liệu từ nhiều nguồn; báo cáo Bộ Công an theo thủ tục khai báo biến động quy mô tích tụ dữ liệu quy định tại khoản 2 Điều 20 của Luật này trước khi kết hợp dữ liệu quy mô lớn thuộc dữ liệu Cấp độ 3, dữ liệu Cấp độ 4.

3. Tổ chức, cá nhân trong nước và nước ngoài vận hành nền tảng mạng xã hội, sàn giao dịch thương mại điện tử, dịch vụ điện toán đám mây hoặc dịch vụ số khác có hoạt động xử lý dữ liệu quy mô lớn đối với người dùng tại Việt Nam đều thuộc đối tượng áp dụng Điều này theo quy định tại điểm c khoản 2 Điều 1 của Luật này.

4. Việc phối hợp áp dụng biện pháp an ninh mạng và biện pháp an ninh dữ liệu đối với hệ thống thông tin xử lý dữ liệu quy mô lớn thực hiện thống nhất,

tích hợp trong cùng hồ sơ, không tổ chức hai đợt thẩm định, đánh giá riêng biệt đối với cùng một hệ thống, cùng một nội dung, theo nguyên tắc áp dụng pháp luật quy định tại khoản 3 Điều 1 của Luật này.

5. Chính phủ quy định chi tiết ngưỡng định lượng xử lý dữ liệu quy mô lớn, tiêu chuẩn kỹ thuật ẩn danh hóa, giả danh hóa và cơ chế phối hợp áp dụng biện pháp an ninh mạng, an ninh dữ liệu quy định tại Điều này.

Điều 12. Bảo vệ an ninh dữ liệu trong phát triển kinh tế số, Chính phủ số và các lĩnh vực quốc gia trọng yếu

1. Tổ chức, cá nhân tham gia thị trường dữ liệu, sàn dữ liệu, kinh doanh dịch vụ dữ liệu có nghĩa vụ xác định cấp độ rủi ro và áp dụng biện pháp bảo vệ an ninh dữ liệu tương ứng cấp độ, quy mô, mức độ rủi ro theo Điều 8 của Luật này.

2. Dữ liệu phục vụ hoạt động của cơ quan nhà nước, dịch vụ công trực tuyến và dữ liệu vận hành hạ tầng kỹ thuật thuộc lĩnh vực quốc gia trọng yếu (tài chính - ngân hàng, năng lượng, y tế, giáo dục, viễn thông, giao thông vận tải, hạ tầng tính toán trí tuệ nhân tạo) có quy mô lớn hoặc phạm vi ảnh hưởng liên vùng, liên ngành theo tiêu chí quy định tại khoản 4 Điều này là đối tượng ưu tiên đưa vào Danh mục dữ liệu quan trọng, Danh mục dữ liệu cốt lõi để xác định Cấp độ 3, Cấp độ 4 theo Điều 8 của Luật này.

3. Hệ thống thông tin phục vụ Chính phủ số, lĩnh vực trọng yếu thuộc dữ liệu Cấp độ 3, Cấp độ 4 thực hiện nghĩa vụ kết nối, chia sẻ thông tin giám sát với Hệ thống giám sát an ninh dữ liệu tập trung quốc gia theo quy định tại khoản 1 Điều 18 của Luật này; dữ liệu quân sự do Bộ Quốc phòng chủ trì giám sát. Chủ quản hệ thống thực hiện kiểm toán cấu hình an ninh, rà quét lỗ hổng bảo mật tối thiểu 02 lần một năm; xây dựng phương án dự phòng thảm họa, bảo đảm năng lực khôi phục dữ liệu sạch sau sự cố.

4. Chính phủ quy định chi tiết tiêu chí xác định quy mô lớn, phạm vi ảnh hưởng liên vùng, liên ngành quy định tại khoản 2 Điều này và lộ trình phân kỳ thực hiện Điều này.

Điều 13. Bảo vệ an ninh dữ liệu đối với hạ tầng số và dịch vụ viễn thông, Internet

1. Doanh nghiệp cung cấp dịch vụ viễn thông, dịch vụ Internet, dịch vụ mạng lõi và doanh nghiệp cung cấp hạ tầng dữ liệu tại Việt Nam có trách nhiệm áp dụng biện pháp bảo đảm an ninh, toàn vẹn, sẵn sàng của luồng dữ liệu truyền dẫn; triển khai hệ thống kỹ thuật rà quét, phát hiện, ngăn chặn sự cố mất an ninh dữ liệu, tấn công mạng, rò rỉ dữ liệu xuyên biên giới; lưu trữ nhật ký kết nối mạng, nhật ký hệ thống theo thời hạn thống nhất quy định tại khoản 4 Điều 20 của Luật này; thực hiện ngăn chặn khẩn cấp, bóc gỡ dữ liệu

độc hại, dữ liệu xâm phạm an ninh quốc gia khi có yêu cầu bằng văn bản của Bộ Công an.

2. Doanh nghiệp cung cấp hạ tầng dữ liệu, trung tâm dữ liệu tập trung quy mô lớn phục vụ xử lý dữ liệu Cấp độ 3, dữ liệu Cấp độ 4 hoặc hạ tầng tính toán trí tuệ nhân tạo có trách nhiệm:

a) Áp dụng tiêu chuẩn kỹ thuật về trung tâm dữ liệu xanh, tối ưu hóa chỉ số hiệu quả sử dụng điện năng, nước làm mát và từng bước nâng cao tỷ lệ sử dụng năng lượng tái tạo;

b) Xây dựng, định kỳ kiểm tra phương án dự phòng năng lượng tại chỗ, bảo đảm duy trì hoạt động tối thiểu của hệ thống lưu trữ dữ liệu trọng yếu khi xảy ra sự cố sụt giảm hoặc mất điện lưới diện rộng;

c) Báo cáo đánh giá rủi ro an toàn hạ tầng vật lý và an ninh năng lượng định kỳ hằng năm gửi Bộ Công an và Bộ Công Thương; báo cáo quy định tại điểm này là báo cáo chuyên ngành năng lượng, thực hiện độc lập với thủ tục hành chính về an ninh dữ liệu quy định tại khoản 7 Điều 23 của Luật này.

3. Doanh nghiệp nước ngoài cung cấp dịch vụ viễn thông, Internet xuyên biên giới có hoạt động xử lý dữ liệu người dùng tại Việt Nam thực hiện nghĩa vụ quy định tại khoản 1 Điều này; điều kiện lưu trữ dữ liệu và đặt chi nhánh hoặc văn phòng đại diện thực hiện theo pháp luật về an ninh mạng và pháp luật có liên quan, chỉ bổ sung yêu cầu an ninh dữ liệu đặc thù theo Luật này.

4. Doanh nghiệp vi phạm quy định tại Điều này, không tuân thủ lệnh điều phối ứng phó khẩn cấp hoặc để xảy ra rò rỉ dữ liệu quy mô lớn, tùy tính chất, mức độ vi phạm, bị áp dụng biện pháp cưỡng chế kỹ thuật theo quy định tại Điều 19 của Luật này.

5. Chính phủ quy định chi tiết yêu cầu kỹ thuật rà quét, phát hiện, ngăn chặn sự cố quy định tại khoản 1 Điều này; tiêu chuẩn trung tâm dữ liệu xanh, chỉ số hiệu quả sử dụng năng lượng quy định tại khoản 2 Điều này.

Điều 14. Thẩm định an ninh dữ liệu trong hoạt động đầu tư, chuyển giao công nghệ

1. Việc thẩm định an ninh dữ liệu đối với hệ thống thông tin, dự án đầu tư, chuyển giao công nghệ có cấu phần xử lý dữ liệu Cấp độ 4, dữ liệu Cấp độ 3 thực hiện như sau:

a) Đối với dữ liệu Cấp độ 4: Bộ Công an thẩm định đầy đủ trước khi phê duyệt dự án và trước khi đưa hệ thống vào vận hành;

b) Đối với dữ liệu Cấp độ 3: chủ quản hệ thống tự đánh giá, đăng ký và được đưa vào vận hành; chịu hậu kiểm định kỳ hoặc theo tỷ lệ chọn mẫu tối

thiểu 20% số hệ thống đã đăng ký mỗi năm. Bộ Công an chỉ thẩm định trước khi vận hành khi hệ thống, dự án có dấu hiệu rủi ro cao trên cơ sở tiêu chí quy định tại khoản 2 Điều 8 của Luật này.

2. Văn bản thẩm định đối với dữ liệu Cấp độ 4 là căn cứ bắt buộc trong hồ sơ quyết định đầu tư, chuyển giao công nghệ; thẩm định trước khi phê duyệt dự án và thẩm định trước khi vận hành là hai thủ tục độc lập, không thay thế lẫn nhau.

3. Việc thẩm định an ninh dữ liệu quy định tại Điều này được tích hợp, phối hợp thực hiện cùng thẩm định an ninh mạng theo nguyên tắc quy định tại khoản 4 Điều 11 của Luật này.

4. Cơ quan thẩm định có trách nhiệm bảo mật thông tin kỹ thuật, mã nguồn, bí mật kinh doanh do tổ chức cung cấp, chỉ sử dụng cho mục đích thẩm định an ninh dữ liệu. Tổ chức thực hiện hành vi khai báo sai cấp độ rủi ro quy định tại khoản 5 Điều 5 của Luật này nhằm né tránh nghĩa vụ thẩm định trước khi vận hành quy định tại điểm a khoản 1 Điều này thì bị buộc dừng vận hành đến khi hoàn thành thẩm định, đồng thời bị xử lý theo Điều 23 của Luật này.

5. Chính phủ quy định chi tiết nội dung, trình tự, thủ tục, thời hạn thẩm định quy định tại Điều này; quy định cơ chế thực hiện hậu kiểm bảo đảm tỷ lệ tối thiểu quy định tại điểm b khoản 1 Điều này.

Điều 15. Bảo vệ an ninh dữ liệu đối với công nghệ mới, trí tuệ nhân tạo

1. Dữ liệu Cấp độ 4, dữ liệu Cấp độ 3 có ý nghĩa chiến lược quốc gia, dữ liệu chứa bí mật nhà nước phải áp dụng biện pháp bảo mật dài hạn, có khả năng phòng vệ trước điện toán lượng tử và công nghệ mới; Nhà nước khuyến khích tổ chức xây dựng lộ trình chuyển đổi sang mật mã kháng lượng tử. Đối với hệ thống lưu trữ, xử lý dữ liệu Cấp độ 4 thuộc cơ quan Đảng, Nhà nước và lực lượng vũ trang, việc chuyển đổi hoàn thành chậm nhất vào ngày 01 tháng 01 năm 2035 theo lộ trình do Thủ tướng Chính phủ quyết định trên cơ sở đề xuất của Bộ Công an và Ban Cơ yếu Chính phủ. Đối với dữ liệu chứa bí mật nhà nước, Ban Cơ yếu Chính phủ chủ trì, phối hợp Bộ Công an, Bộ Quốc phòng tham mưu Thủ tướng Chính phủ lộ trình chuyển đổi mật mã kháng lượng tử.

2. Tổ chức, doanh nghiệp nghiên cứu, phát triển, vận hành, cung cấp dịch vụ trí tuệ nhân tạo, đặc biệt là hệ thống trí tuệ nhân tạo tạo sinh, có trách nhiệm bảo đảm an ninh, toàn vẹn dữ liệu huấn luyện như sau:

a) Áp dụng biện pháp phù hợp mức độ rủi ro để quản lý, kiểm chứng nguồn gốc dữ liệu huấn luyện; không sử dụng dữ liệu có nguồn gốc bất hợp pháp mà tổ chức biết hoặc buộc phải biết;

b) Kiểm soát truy cập, ghi nhật ký thao tác đối với dữ liệu huấn luyện, bảo đảm khả năng truy xuất nguồn gốc;

c) Giám sát, áp dụng biện pháp phòng ngừa để phát hiện, ngăn chặn hành vi chèn dữ liệu độc hại, đầu độc dữ liệu huấn luyện làm sai lệch mô hình.

Việc phân loại rủi ro hệ thống trí tuệ nhân tạo, thử nghiệm có kiểm soát, giám sát của con người và gắn nhãn nội dung do trí tuệ nhân tạo tạo ra không thuộc phạm vi điều chỉnh của Luật này, thực hiện theo pháp luật về trí tuệ nhân tạo theo nguyên tắc phân định pháp luật quy định tại Điều 1 của Luật này.

3. Khi phát hiện dấu hiệu tấn công đầu độc dữ liệu huấn luyện hoặc hành vi xâm phạm dữ liệu thuộc phạm vi điều chỉnh của Luật này dẫn đến hệ thống trí tuệ nhân tạo đưa ra thông tin sai lệch về chủ quyền, lịch sử, biên giới, văn hóa của Việt Nam, Bộ Công an có quyền yêu cầu tổ chức, doanh nghiệp giải trình, khắc phục trong thời hạn xác định. Trường hợp vi phạm nghiêm trọng gây hậu quả đặc biệt lớn, phát sinh trực tiếp từ hành vi xâm phạm, đầu độc, làm sai lệch dữ liệu thuộc phạm vi điều chỉnh của Luật này, Bộ Công an quyết định bằng văn bản việc tạm ngừng sử dụng tập dữ liệu huấn luyện vi phạm hoặc tạm ngừng cung cấp dịch vụ theo trình tự, thủ tục và bảo đảm các quyền quy định tại khoản 3 Điều 19 của Luật này; thời hạn áp dụng không quá 30 ngày cho mỗi lần quyết định, được gia hạn nhưng tổng thời hạn không quá 60 ngày. Cơ quan, người có thẩm quyền không yêu cầu tổ chức, doanh nghiệp bàn giao mã nguồn thô hoặc trọng số mô hình trong quá trình yêu cầu giải trình, kiểm tra hành chính theo khoản này, trừ trường hợp phục vụ điều tra vụ án hình sự theo quyết định của cơ quan tiến hành tố tụng; cơ quan tiếp nhận thông tin có trách nhiệm bảo mật bí mật kinh doanh, bí mật công nghệ của tổ chức, doanh nghiệp theo quy định của pháp luật.

4. Hệ thống trí tuệ nhân tạo dùng dữ liệu Cấp độ 3, dữ liệu Cấp độ 4 để ra quyết định tự động trong y tế, tín dụng, tuyển dụng, giao thông, giáo dục phải được kiểm thử độc lập, giám sát và bảo đảm quyền con người được xem xét lại quyết định tự động; quyền được xem xét lại quyết định tự động quy định tại khoản này được thực hiện trong phạm vi bảo đảm an ninh dữ liệu, không thay thế quyền của chủ thể dữ liệu cá nhân theo pháp luật về bảo vệ dữ liệu cá nhân đối với trường hợp dữ liệu được xử lý là dữ liệu cá nhân. Bộ Công an thẩm định nội dung liên quan đến an ninh dữ liệu.

5. Chính phủ quy định chi tiết danh mục dữ liệu Cấp độ 3 có ý nghĩa chiến lược quốc gia quy định tại khoản 1 Điều này; lộ trình chuyển đổi mật mã kháng lượng tử đối với chủ thể ngoài phạm vi quy định tại khoản 1 Điều này; tiêu chuẩn kỹ thuật và khung trách nhiệm quy định tại Điều này.

6. Trường hợp hệ thống trí tuệ nhân tạo đồng thời thuộc đối tượng quản lý hệ thống rủi ro cao theo quy định của pháp luật trí tuệ nhân tạo và xử lý dữ liệu Cấp độ 3, Cấp độ 4, hồ sơ đánh giá tác động an ninh dữ liệu quy định tại Điều 10 của Luật này được tích hợp trong hồ sơ đánh giá rủi ro theo Luật Trí tuệ nhân

tạo. Việc báo cáo, xử lý sự cố liên quan đến dữ liệu huấn luyện thực hiện theo Điều 20 của Luật này; việc báo cáo, xử lý sự cố khác của hệ thống trí tuệ nhân tạo thực hiện theo pháp luật về trí tuệ nhân tạo.

Điều 16. Bảo vệ an ninh dữ liệu trong chuỗi cung ứng

1. Tổ chức, cá nhân vận hành, xử lý dữ liệu có trách nhiệm kiểm soát an ninh dữ liệu đối với bên thứ ba tham gia chuỗi cung ứng, bao gồm nhà cung cấp dịch vụ điện toán đám mây, dịch vụ trí tuệ nhân tạo, đơn vị vận hành trung tâm dữ liệu, bên môi giới dữ liệu, bên nhận thuê ngoài xử lý dữ liệu và các bên thứ ba khác có quyền tiếp cận, lưu trữ hoặc xử lý dữ liệu.

2. Trước khi thiết lập quan hệ hợp tác với bên thứ ba tiếp cận, lưu trữ hoặc xử lý dữ liệu Cấp độ 3, dữ liệu Cấp độ 4 hoặc dữ liệu quy mô lớn, và định kỳ hằng năm trong quá trình hợp tác, tổ chức, cá nhân phải đánh giá rủi ro an ninh dữ liệu đối với bên thứ ba về năng lực kỹ thuật, nguy cơ, lỗ hổng bảo mật và biện pháp giảm thiểu, phương án ứng phó sự cố. Đối với dữ liệu Cấp độ 1, Cấp độ 2 không thuộc quy mô lớn, tổ chức, cá nhân tự quyết định mức độ, tần suất đánh giá phù hợp, không bắt buộc thực hiện theo trình tự quy định tại khoản này.

3. Việc chia sẻ, chuyển giao hoặc cho phép bên thứ ba tiếp cận dữ liệu Cấp độ 3, dữ liệu Cấp độ 4 hoặc dữ liệu quy mô lớn chỉ được thực hiện sau khi ký hợp đồng an ninh dữ liệu quy định tại khoản 23 Điều 2 của Luật này hoặc điều khoản bảo mật dữ liệu bắt buộc trong hợp đồng dịch vụ, quy định rõ phạm vi, mục đích xử lý, giới hạn quyền truy cập, trách nhiệm kỹ thuật, nghĩa vụ thông báo trong không quá 24 giờ khi xảy ra hoặc có nguy cơ xảy ra sự cố rò rỉ dữ liệu và trách nhiệm bồi thường thiệt hại; đối với dữ liệu Cấp độ 1, Cấp độ 2 không thuộc quy mô lớn, tổ chức, cá nhân thỏa thuận nội dung bảo mật phù hợp trong hợp đồng dịch vụ theo quy định chung của pháp luật dân sự, thương mại.

4. Tổ chức, cá nhân có quyền kiểm toán định kỳ, đột xuất hệ thống an ninh dữ liệu của bên thứ ba tiếp cận, lưu trữ hoặc xử lý dữ liệu Cấp độ 3, dữ liệu Cấp độ 4 hoặc dữ liệu quy mô lớn, hoặc yêu cầu báo cáo kiểm toán độc lập để chứng minh khả năng tuân thủ tiêu chuẩn an ninh dữ liệu đã cam kết.

5. Nghĩa vụ bảo vệ an ninh dữ liệu áp dụng đối với bên xử lý dữ liệu được giới hạn trong phạm vi hoạt động xử lý dữ liệu được ủy quyền, giao kết hợp đồng, phù hợp khả năng kiểm soát thực tế đối với nội dung, mục đích xử lý dữ liệu; được thực hiện thống nhất theo trách nhiệm của chủ quản dữ liệu quy định tại khoản 2 Điều 6 và nghĩa vụ đối với bên thứ ba tham gia chuỗi cung ứng quy định tại các khoản 1, 2, 3 và 4 Điều này. Nghĩa vụ đòi hỏi hiểu biết về nội dung, mục đích xử lý dữ liệu mà bên xử lý dữ liệu không có khả năng thực hiện độc lập trong phạm vi được ủy quyền, giao kết hợp đồng thuộc trách nhiệm của chủ sở hữu dữ liệu hoặc chủ quản dữ liệu.

6. Chính phủ quy định chi tiết nội dung tối thiểu của hợp đồng an ninh dữ liệu hoặc điều khoản bảo mật dữ liệu bắt buộc quy định tại khoản 3 Điều này; phương pháp, tiêu chí đánh giá rủi ro an ninh dữ liệu đối với bên thứ ba quy định tại khoản 2 Điều này; trình tự, thủ tục kiểm toán quy định tại khoản 4 Điều này.

Điều 17. Bảo vệ an ninh dữ liệu trong lưu chuyển dữ liệu xuyên biên giới

1. Hoạt động chuyển dữ liệu ra nước ngoài thực hiện theo nguyên tắc phân luồng rủi ro, bảo đảm tối ưu hóa lợi ích kinh tế và không xâm phạm an ninh quốc gia, chủ quyền số. Dữ liệu Cấp độ 4 về biên giới, chủ quyền lãnh thổ, công trình quân sự, quốc phòng; dữ liệu mật mã cơ yếu, dữ liệu bảo vệ hạ tầng thông tin trọng yếu; dữ liệu định danh sinh trắc học quy mô lớn của công dân bị cấm chuyển ra nước ngoài, trừ trường hợp đặc biệt phục vụ lợi ích quốc gia đặc biệt quan trọng về đối ngoại, quốc phòng hoặc hợp tác quốc tế theo cam kết của Nhà nước, được Thủ tướng Chính phủ cho phép bằng văn bản theo trình tự, thủ tục do Chính phủ quy định.

2. Dữ liệu Cấp độ 4 thuộc trường hợp được phép chuyển ra nước ngoài quy định tại khoản 1 Điều này phải được Bộ Công an thẩm định, cấp văn bản chấp thuận trước khi chuyển. Dữ liệu Cấp độ 3 áp dụng cơ chế thông báo trước tối thiểu 15 ngày, không phải chờ chấp thuận, trừ khi Bộ Công an yêu cầu tạm dừng bằng văn bản khi phát hiện rủi ro nghiêm trọng có căn cứ rõ ràng về nguy cơ xâm phạm an ninh quốc gia, nguy cơ lộ lọt dữ liệu quy mô lớn hoặc vi phạm cam kết bảo vệ dữ liệu của bên tiếp nhận, theo trình tự, thủ tục và bảo đảm các quyền quy định tại khoản 3 Điều 19 của Luật này; thời hạn tạm dừng không quá 30 ngày kể từ ngày ra văn bản, được gia hạn một lần không quá 30 ngày nếu rủi ro chưa được khắc phục. Dữ liệu là bí mật kinh doanh không phải thẩm định trước nếu quốc gia tiếp nhận được công nhận có hệ thống pháp luật bảo vệ dữ liệu tương đương, hoặc các bên ký hợp đồng tiêu chuẩn về bảo vệ dữ liệu, hoặc chủ thể chuyển giao đã được cấp chứng nhận hợp quy về an ninh dữ liệu theo khoản 5 Điều 10 của Luật này đối với sản phẩm, dịch vụ sử dụng để bảo vệ dữ liệu được chuyển giao; tổ chức phải khai báo, tự chịu trách nhiệm về việc xác định dữ liệu là bí mật kinh doanh và chịu hậu kiểm của Bộ Công an. Chính phủ quy định tiêu chí, thẩm quyền công nhận, danh mục quốc gia, vùng lãnh thổ có mức bảo vệ dữ liệu tương đương và mẫu hợp đồng tiêu chuẩn quy định tại khoản này.

3. Dữ liệu được trích xuất từ dữ liệu Cấp độ 4, dữ liệu Cấp độ 3 chỉ thuộc phạm vi hạn chế chuyển ra nước ngoài như dữ liệu gốc khi có khả năng tái tạo, suy ngược hoặc làm lộ dữ liệu gốc theo tiêu chí kỹ thuật do Chính phủ quy định. Hành vi cố ý chuyển đổi, mã hóa, trích xuất đặc trưng từ dữ liệu Cấp độ 4, dữ liệu Cấp độ 3 thuộc trường hợp nêu trên nhằm chuyển ra nước ngoài mà không thực hiện nghĩa vụ thông báo hoặc thẩm định bị coi là hành vi vi phạm và bị xử lý như vi phạm

chuyển dữ liệu trái phép xuyên biên giới. Dữ liệu đã khử nhận dạng theo cách không thể khôi phục dữ liệu gốc không bị áp dụng hạn chế tại khoản này.

4. Việc xác định quy mô tích tụ dữ liệu để tính cấp độ rủi ro và áp dụng điều kiện chuyển dữ liệu xuyên biên giới thực hiện theo quy định tại khoản 9 Điều 8 của Luật này.

5. Dữ liệu Cấp độ 3 có tác động trực tiếp, tức thời đến quốc phòng, an ninh, tài chính - ngân hàng, năng lượng, viễn thông theo tiêu chí định lượng do Chính phủ quy định phải được lưu trữ tại trung tâm dữ liệu trên lãnh thổ Việt Nam; dữ liệu Cấp độ 4 lưu trữ tại hạ tầng dữ liệu quốc gia trọng yếu.

Trường hợp lưu trữ trên điện toán đám mây quốc tế, chủ quản dữ liệu phải duy trì bản sao lưu tại Việt Nam với tần suất tương xứng mức độ rủi ro cụ thể của dữ liệu, bảo đảm cơ quan nhà nước có thẩm quyền được quyền truy cập, kiểm tra, sao lưu dữ liệu khi cần thiết để phục vụ điều tra, ứng phó sự cố hoặc bảo vệ an ninh quốc gia theo trình tự, thủ tục của pháp luật. Trong nhóm dữ liệu quy định tại đoạn 1 khoản này, đối với dữ liệu trực tiếp phục vụ quốc phòng, an ninh hoặc có nguy cơ ảnh hưởng tức thời đến an toàn hệ thống tài chính - ngân hàng, năng lượng, viễn thông ở quy mô quốc gia, chủ quản dữ liệu phải duy trì bản sao lưu thời gian thực; đối với dữ liệu Cấp độ 3 còn lại thuộc phạm vi khoản này, áp dụng tần suất sao lưu tối thiểu do Chính phủ quy định. Dữ liệu Cấp độ 4 không áp dụng ngoại lệ lưu trữ trên điện toán đám mây quốc tế quy định tại khoản này.

Chính phủ quy định lộ trình phân kỳ áp dụng yêu cầu sao lưu quy định tại khoản này trên cơ sở đánh giá chi phí, tính khả thi kỹ thuật và quy mô của từng nhóm đối tượng.

6. Trường hợp dữ liệu chuyển ra nước ngoài đồng thời là dữ liệu cá nhân và là dữ liệu Cấp độ 3, dữ liệu Cấp độ 4 thì tổ chức chỉ thực hiện một thủ tục duy nhất theo Điều này, tích hợp nội dung bảo vệ quyền chủ thể dữ liệu cá nhân trong cùng hồ sơ. Doanh nghiệp nước ngoài vi phạm quy định tại Điều này, đã được cảnh báo bằng văn bản và không khắc phục trong thời hạn được ấn định, tùy tính chất, mức độ vi phạm, bị Bộ Công an quyết định áp dụng biện pháp cưỡng chế thiết lập hạ tầng, lưu trữ dữ liệu tại Việt Nam hoặc biện pháp kỹ thuật ngăn chặn tương xứng mức độ vi phạm theo trình tự, thủ tục và bảo đảm các quyền quy định tại khoản 3 Điều 19 của Luật này; thời hạn thực hiện không quá 06 tháng kể từ ngày quyết định có hiệu lực, được gia hạn một lần không quá 06 tháng trong trường hợp cần thiết.

7. Nhà nước áp dụng cơ chế hậu kiểm đối với dữ liệu nhập khẩu, tiếp nhận từ nước ngoài để lưu trữ, xử lý trên lãnh thổ Việt Nam. Tổ chức, cá nhân tiếp nhận dữ liệu có trách nhiệm tự đánh giá, phân loại dữ liệu trước khi đưa vào lưu trữ, xử lý; áp dụng biện pháp phát hiện dữ liệu không rõ nguồn

gốc, dữ liệu độc hại hoặc dữ liệu bị đầu độc quy định tại khoản 18, khoản 20 Điều 2 của Luật này; khi phát hiện hoặc có căn cứ rõ ràng về việc dữ liệu tiếp nhận thuộc các trường hợp nêu trên, phải dừng ngay việc lưu trữ, xử lý đối với phần dữ liệu bị nghi ngờ và báo cáo Bộ Công an theo Điều 20 của Luật này. Bộ Công an thực hiện giám sát, thanh tra, kiểm tra việc tuân thủ nghĩa vụ quy định tại khoản này; trường hợp phát hiện vi phạm nghiêm trọng, có quyền áp dụng biện pháp cưỡng chế kỹ thuật quy định tại khoản 17 Điều 2 và Điều 19 của Luật này. Chính phủ quy định chi tiết tiêu chí, phương pháp phát hiện, biện pháp cách ly, xử lý và trình tự thực hiện đối với dữ liệu nhập khẩu thuộc trường hợp quy định tại khoản này.

8. Các biện pháp hạn chế lưu trữ, chuyển giao dữ liệu xuyên biên giới quy định tại Điều này được áp dụng trong phạm vi thực sự cần thiết, tương xứng mức độ rủi ro, không phân biệt đối xử giữa tổ chức trong nước và nước ngoài, phù hợp với các điều khoản ngoại lệ an ninh tại điều ước quốc tế mà nước Cộng hòa xã hội chủ nghĩa Việt Nam là thành viên.

CHƯƠNG IV
GIÁM SÁT, PHÒNG NGỪA VÀ ỨNG PHÓ SỰ CỐ AN NINH DỮ LIỆU

Điều 18. Giám sát an ninh dữ liệu tập trung và cảnh báo sớm rủi ro an ninh dữ liệu

1. Trung tâm Quản trị an ninh dữ liệu quốc gia thực hiện giám sát, phân tích, cảnh báo sớm và hỗ trợ ngăn chặn hành vi xâm phạm dữ liệu trái phép. Chủ quản hệ thống thông tin xử lý dữ liệu Cấp độ 4 truyền nhật ký an ninh qua thiết bị một chiều; chủ quản hệ thống thông tin xử lý dữ liệu Cấp độ 3 kết nối, chia sẻ thông tin cảnh báo an ninh theo quy chuẩn kỹ thuật, trừ hệ thống thông tin quân sự do Bộ Quốc phòng quản lý, thực hiện phối hợp, chia sẻ thông tin cảnh báo nguy cơ với Bộ Công an theo quy chế phối hợp quy định tại khoản 3 Điều này, không bắt buộc kết nối, tích hợp kỹ thuật với hệ thống giám sát an ninh dữ liệu tập trung quốc gia. Nội dung truyền, chia sẻ về hệ thống giám sát tập trung là siêu dữ liệu an ninh và nhật ký sự kiện, không bao gồm nội dung dữ liệu; việc trích xuất nội dung dữ liệu cụ thể thực hiện theo quy định tại khoản 2 Điều này.

2. Hoạt động giám sát phải bảo đảm bí mật nghiệp vụ; nghiêm cấm lợi dụng chức năng giám sát để can thiệp trái phép. Việc trích xuất nội dung dữ liệu cụ thể chỉ được thực hiện trong trường hợp khẩn cấp về an ninh quốc gia hoặc phục vụ điều tra theo trình tự, thủ tục của pháp luật tố tụng hình sự; thẩm quyền, trình tự, thủ tục trích xuất, mục đích sử dụng, thời hạn lưu giữ và phạm vi chủ

thể được tiếp cận nội dung dữ liệu đã trích xuất thực hiện theo quy định của pháp luật về tố tụng hình sự và quy định chi tiết của Chính phủ.

3. Bộ Công an chủ trì, phối hợp Bộ Quốc phòng xây dựng, vận hành hệ thống cảnh báo sớm rủi ro an ninh dữ liệu quốc gia; Bộ Quốc phòng chủ trì đối với dữ liệu quân sự và chia sẻ thông tin nguy cơ với Bộ Công an.

4. Chủ quản hệ thống lưu trữ, xử lý dữ liệu Cấp độ 4, dữ liệu Cấp độ 3 khi nhận cảnh báo phải triển khai ngay biện pháp cô lập, chặn lọc và báo cáo kết quả khắc phục; nghiêm cấm che giấu hoặc không thực hiện lệnh điều phối ứng phó khẩn cấp.

5. Hệ thống giám sát an ninh dữ liệu tập trung quốc gia phải bảo đảm an ninh, bảo mật đối với dữ liệu, nhật ký tiếp nhận; cơ quan vận hành chịu trách nhiệm khi để xảy ra rò rỉ, lạm dụng. Trường hợp cơ quan nhà nước, người có thẩm quyền trong quá trình giám sát, thanh tra, kiểm tra, áp dụng biện pháp kỹ thuật gây thiệt hại cho cơ quan, tổ chức, cá nhân thì việc bồi thường thực hiện theo pháp luật về trách nhiệm bồi thường của Nhà nước.

6. Chính phủ quy định chi tiết quy chuẩn kỹ thuật kết nối, truyền nhật ký và chia sẻ thông tin cảnh báo an ninh quy định tại Điều này.

Điều 19. Biện pháp kỹ thuật khẩn cấp và nguyên tắc áp dụng biện pháp hạn chế quyền trong bảo vệ an ninh dữ liệu

1. Trong tình huống khẩn cấp đe dọa trực tiếp chủ quyền dữ liệu, an ninh quốc gia, Bộ Công an, Bộ Quốc phòng theo thẩm quyền quản lý nhà nước quy định tại Điều 23 của Luật này, có quyền ban hành lệnh điều phối đặc biệt, áp dụng biện pháp kỹ thuật khẩn cấp quy định tại khoản 3 Điều này đối với doanh nghiệp cung cấp hạ tầng, dịch vụ mạng liên quan.

2. Việc trưng dụng hạ tầng, tài sản, nhân lực trong tình huống khẩn cấp thực hiện theo pháp luật về trưng mua, trưng dụng tài sản.

3. Biện pháp kỹ thuật khẩn cấp và biện pháp hạn chế quyền quy định tại Luật này (cưỡng chế kỹ thuật theo quy định tại khoản 17 Điều 2 của Luật này; tạm ngừng cung cấp dịch vụ; bóc gỡ dữ liệu; buộc dừng vận hành; buộc thiết lập hạ tầng, lưu trữ dữ liệu tại Việt Nam và các biện pháp hạn chế quyền khác quy định tại Luật này) chỉ được áp dụng khi có căn cứ do Luật này quy định, bảo đảm các yêu cầu sau:

a) Tương xứng với mức độ nguy hiểm, đe dọa;

b) Do người có thẩm quyền quyết định bằng văn bản, nêu rõ căn cứ, phạm vi dữ liệu, hệ thống, dịch vụ bị tác động và thời hạn áp dụng;

c) Được thông báo trước cho đối tượng bị áp dụng; trường hợp khẩn cấp, được áp dụng ngay và hoàn thiện quyết định bằng văn bản, thông báo cho đối tượng bị áp dụng trong thời gian sớm nhất sau khi áp dụng;

d) Bảo đảm quyền giải trình, khiếu nại, khởi kiện của đối tượng bị áp dụng;

đ) Được thay đổi, bãi bỏ ngay khi căn cứ áp dụng không còn;

e) Thời hạn áp dụng mỗi biện pháp không quá 30 ngày kể từ ngày quyết định có hiệu lực, được gia hạn nhưng tổng thời hạn không quá 90 ngày; riêng biện pháp kỹ thuật khẩn cấp áp dụng trong tình huống quy định tại khoản 1 Điều này, mỗi lệnh điều phối đặc biệt có thời hạn không quá 30 ngày, được gia hạn nhiều lần nếu tình huống khẩn cấp chưa được khống chế, nhưng mỗi lần gia hạn phải có văn bản đánh giá lại tình huống của cấp có thẩm quyền quy định tại khoản 1 Điều này; tổng thời hạn áp dụng liên tục không quá 180 ngày kể từ lệnh điều phối đặc biệt đầu tiên, trường hợp tình huống khẩn cấp chưa được khống chế khi hết thời hạn này thì phải báo cáo Thủ tướng Chính phủ xem xét, quyết định việc tiếp tục áp dụng.

4. Việc áp dụng biện pháp trái pháp luật gây thiệt hại thì phải bồi thường theo quy định của pháp luật về trách nhiệm bồi thường của Nhà nước. Chính phủ quy định chi tiết trình tự, thủ tục, biểu mẫu và cơ chế phối hợp ban hành, bãi bỏ các biện pháp quy định tại Điều này.

Điều 20. Điều phối ứng cứu, truy vết, điều tra và phục hồi dữ liệu sau sự cố

1. Chủ quản hệ thống thông tin xử lý dữ liệu Cấp độ 2, dữ liệu Cấp độ 3, dữ liệu Cấp độ 4 có nghĩa vụ xây dựng phương án ứng phó sự cố và tổ chức diễn tập định kỳ hằng năm. Bộ Công an, Bộ Quốc phòng chủ trì xây dựng kịch bản mẫu quốc gia, tổ chức diễn tập đối với hạ tầng dữ liệu quốc gia trọng yếu và chỉ huy điều phối khi sự cố được phân loại từ mức nghiêm trọng trở lên.

2. Chủ quản dữ liệu có trách nhiệm báo cáo cho Bộ Công an (đối với dữ liệu quân sự, báo cáo cho Bộ Quốc phòng) và thông báo cho chủ thể dữ liệu bị ảnh hưởng đối với sự cố an ninh dữ liệu liên quan đến dữ liệu Cấp độ 3, dữ liệu Cấp độ 4, hoặc sự cố khác có quy mô ảnh hưởng lớn, xâm phạm quyền, lợi ích hợp pháp của nhiều chủ thể dữ liệu theo tiêu chí do Chính phủ quy định, trong thời hạn do Chính phủ quy định, bảo đảm báo cáo đầy đủ chậm nhất 72 giờ kể từ khi biết hoặc buộc phải biết về sự cố; đối với sự cố an ninh dữ liệu không thuộc trường hợp phải báo cáo, chủ quản dữ liệu tự xử lý, khắc phục và lập, lưu hồ sơ để cung cấp cho cơ quan có thẩm quyền khi có yêu cầu kiểm tra, thanh tra. Việc báo cáo, khai báo an ninh dữ liệu được tiếp nhận qua một đầu mối duy nhất, áp dụng chung cho báo cáo sự cố, khai báo thay đổi cấp độ rủi ro an ninh dữ liệu, khai báo biến động quy mô tích tụ dữ liệu và đề nghị xác nhận đủ điều kiện an

ninh khi khôi phục kết nối hệ thống sau sự cố; nội dung đã báo cáo được sử dụng chung, không báo cáo trùng lặp.

3. Trung tâm Quản trị an ninh dữ liệu quốc gia thuộc Bộ Công an là đầu mối chỉ huy, điều phối ứng cứu sự cố trên phạm vi toàn quốc; Bộ Quốc phòng chủ trì ứng cứu sự cố đối với dữ liệu quân sự, quốc phòng. Trường hợp sự cố xảy ra trên hạ tầng lưỡng dụng, đầu mối chỉ huy được xác định theo tính chất chủ yếu của sự cố; các cơ quan liên quan thông báo, phối hợp ngay khi phát hiện sự cố, bảo đảm không có khoảng trống hoặc chồng chéo chỉ huy.

4. Cơ quan chuyên trách thu thập dữ liệu điện tử, trích xuất nhật ký hệ thống phục vụ truy vết, điều tra theo trình tự, thủ tục của pháp luật tố tụng; dữ liệu điện tử được thu thập là nguồn chứng cứ, giá trị chứng cứ được xác định theo quy định của pháp luật về tố tụng và pháp luật về giao dịch điện tử. Doanh nghiệp viễn thông, công nghệ thông tin, dịch vụ Internet, dịch vụ mạng lõi và doanh nghiệp cung cấp hạ tầng dữ liệu bảo đảm tính toàn vẹn nhật ký kết nối mạng, nhật ký hệ thống (không bao gồm nội dung dữ liệu truyền tải) và lưu trữ trong thời hạn thống nhất là 12 tháng, trừ trường hợp có văn bản đóng băng, phong tỏa dữ liệu điện tử phục vụ điều tra vụ án hình sự cụ thể của cơ quan có thẩm quyền. Sau khi sự cố được khống chế, chủ quản dữ liệu khôi phục hệ thống, loại bỏ mã độc, khắc phục lỗ hổng trước khi đưa hệ thống trở lại vận hành; đối với hệ thống của cơ quan nhà nước và hạ tầng trọng yếu, việc khôi phục kết nối phải có văn bản xác nhận đủ điều kiện an ninh của Bộ Công an hoặc Bộ Quốc phòng, căn cứ trên kết quả khắc phục lỗ hổng, loại bỏ mã độc và kiểm tra kỹ thuật theo tiêu chuẩn do Chính phủ quy định; cơ quan có thẩm quyền phải trả lời bằng văn bản trong thời hạn không quá 05 ngày làm việc kể từ ngày nhận đủ hồ sơ đề nghị xác nhận, quá thời hạn mà không có văn bản từ chối thì hệ thống được coi là đủ điều kiện khôi phục kết nối.

5. Chính phủ quy định chi tiết tiêu chí phân loại cấp độ sự cố; tiêu chí xác định sự cố phải báo cáo theo khoản 2 Điều này; quy trình báo cáo và thời hạn báo cáo trong phạm vi không vượt quá thời hạn tối đa quy định tại khoản 2 Điều này; cơ chế điều phối, trưng tập chuyên gia; quy chuẩn kỹ thuật bảo quản dữ liệu điện tử là nguồn chứng cứ và lưu trữ nhật ký quy định tại khoản 4 Điều này.

CHƯƠNG V
PHÁT TRIỂN NGUỒN NHÂN LỰC VÀ QUẢN LÝ NHÀ NƯỚC VỀ AN NINH DỮ LIỆU

Điều 21. Lực lượng bảo vệ, phát triển nguồn nhân lực bảo vệ an ninh dữ liệu

1. Lực lượng chuyên trách bảo vệ an ninh dữ liệu quốc gia gồm: lực lượng chuyên trách thuộc Bộ Công an chủ trì, điều phối tổng thể; lực lượng chuyên trách

thuộc Bộ Quốc phòng chủ trì bảo vệ dữ liệu quân sự, quốc phòng; lực lượng bảo vệ an ninh dữ liệu tại Bộ, ngành, Ủy ban nhân dân cấp tỉnh, cơ quan, tổ chức quản lý trực tiếp hệ thống thông tin, cơ sở dữ liệu quan trọng về an ninh quốc gia; tổ chức, cá nhân được huy động tham gia bảo vệ an ninh dữ liệu. Lực lượng bảo vệ an ninh dữ liệu thuộc lực lượng bảo vệ an ninh mạng. Lực lượng bảo vệ an ninh dữ liệu tại Bộ, ngành, Ủy ban nhân dân cấp tỉnh, cơ quan, tổ chức quy định tại khoản này được bố trí trên cơ sở tổ chức, biên chế hiện có, kiêm nhiệm hoặc chuyên trách theo quy mô, tính chất dữ liệu quản lý, không hình thành tổ chức, biên chế mới ngoài quy định của pháp luật về tổ chức bộ máy; trường hợp phát sinh nhu cầu về tổ chức, biên chế, kinh phí thì thực hiện theo quy định của pháp luật về tổ chức bộ máy nhà nước và pháp luật về ngân sách nhà nước.

2. Nhà nước ưu tiên đầu tư xây dựng lực lượng chuyên trách tiến thẳng lên hiện đại; phát triển mạng lưới cơ sở đào tạo nguồn nhân lực về an ninh dữ liệu phù hợp quy hoạch mạng lưới cơ sở giáo dục đại học theo pháp luật về giáo dục; chính sách học bổng, hỗ trợ đào tạo chuyên sâu đối với nhân lực chất lượng cao về an ninh dữ liệu được thực hiện thông qua Quỹ học bổng quốc gia theo pháp luật về giáo dục hoặc chương trình, đề án cụ thể do cấp có thẩm quyền quyết định.

3. Nhân sự vận hành trực tiếp hệ thống xử lý dữ liệu Cấp độ 3, dữ liệu Cấp độ 4 phải có chứng nhận chuyên môn về an ninh dữ liệu do cơ quan có thẩm quyền cấp hoặc chứng chỉ quốc tế thuộc danh mục do Bộ Công an công bố; nhân sự đã được cấp chứng nhận tập huấn kiến thức, kỹ năng chuyên sâu về an ninh mạng theo quy định của pháp luật về an ninh mạng đối với hệ thống thông tin cùng cấp độ được công nhận đã đáp ứng một phần nội dung chứng nhận chuyên môn về an ninh dữ liệu quy định tại khoản này theo hướng dẫn của Bộ Công an, không phải sát hạch lại nội dung trùng lặp. Nhà nước áp dụng cơ chế đãi ngộ đặc biệt, tuyển dụng đặc cách đối với chuyên gia, nhà khoa học có thành tích xuất sắc, bao gồm người Việt Nam định cư ở nước ngoài; việc bảo vệ chuyên gia độc lập phát hiện, thông báo lỗ hổng bảo mật có thiện chí thực hiện theo quy định tại Điều 22 của Luật này.

4. Cơ quan, tổ chức sử dụng chuyên gia, đối tác nước ngoài tham gia dự án dữ liệu Cấp độ 3, Cấp độ 4 thực hiện thẩm tra an ninh nhân sự, ký thỏa thuận bảo mật, áp dụng giải pháp cách ly kỹ thuật trước khi cho phép truy cập, báo cáo Bộ Công an giải pháp cách ly trước khi nhân sự nước ngoài được phép truy cập dữ liệu Cấp độ 4.

5. Chính phủ quy định chi tiết chức năng, nhiệm vụ, quyền hạn, cơ chế phối hợp của lực lượng chuyên trách; khung tiêu chuẩn năng lực chuyên môn về an ninh dữ liệu đối với nhân sự vận hành trực tiếp quy định tại khoản 3 Điều này (phân biệt với tiêu chuẩn năng lực của nhân sự an ninh dữ liệu chuyên trách và

nhân sự phụ trách an ninh dữ liệu quy định tại khoản 5 Điều 6 của Luật này), điều kiện công nhận chứng chỉ quốc tế, cơ chế đãi ngộ, tuyển dụng đặc cách và quản lý chuyên gia nước ngoài quy định tại Điều này; hồ sơ, thời hạn giải quyết và kết quả của thủ tục xác nhận giải pháp cách ly kỹ thuật đối với chuyên gia nước ngoài quy định tại khoản 4 Điều này.

Điều 22. Huy động nguồn lực xã hội, xã hội hóa tài chính và bảo hiểm rủi ro an ninh dữ liệu

1. Nhà nước khuyến khích tổ chức, cá nhân phát hiện, thông báo lỗ hổng, rủi ro an ninh dữ liệu theo cơ chế bảo vệ quy định tại khoản 2 Điều này; đóng góp giải pháp công nghệ; tham gia đầu tư, tài trợ cho nghiên cứu, phát triển công nghệ, đào tạo nhân lực về an ninh dữ liệu.

2. Người thông báo lỗ hổng, rủi ro an ninh dữ liệu có thiện chí, tuân thủ quy trình, không nhằm trục lợi được bảo vệ danh tính và được xem xét miễn, giảm trách nhiệm hành chính, dân sự đối với hành vi phát hiện, thông báo đó; không áp dụng miễn trừ đối với hành vi khai thác, phát tán, phá hoại dữ liệu.

3. Chi phí đầu tư, tài trợ hợp pháp, có hóa đơn, chứng từ cho hoạt động bảo vệ an ninh dữ liệu quốc gia, nghiên cứu, ứng dụng công nghệ trung tâm dữ liệu xanh, tiết kiệm năng lượng, nghiên cứu công nghệ mật mã thế hệ mới hoặc đào tạo nhân lực được tính là chi phí được trừ khi xác định thu nhập chịu thuế thu nhập doanh nghiệp; việc xác định cụ thể thực hiện theo quy định của pháp luật về thuế thu nhập doanh nghiệp.

4. Doanh nghiệp là chủ quản dữ liệu được khuyến khích mua bảo hiểm rủi ro an ninh dữ liệu tùy theo cấp độ dữ liệu đang lưu trữ, xử lý, thực hiện theo quy định của pháp luật về kinh doanh bảo hiểm. Trường hợp cần thiết xây dựng khung sản phẩm bảo hiểm rủi ro an ninh dữ liệu đặc thù, cơ sở định giá rủi ro và định mức bồi thường riêng, Bộ Tài chính chủ trì, phối hợp Bộ Công an nghiên cứu, đánh giá tác động và báo cáo cấp có thẩm quyền xem xét, quyết định theo quy định của pháp luật về ban hành văn bản quy phạm pháp luật.

5. Nhà nước có chính sách hỗ trợ, ưu đãi đầu tư xây dựng hạ tầng bảo vệ an ninh dữ liệu tại địa bàn có điều kiện kinh tế - xã hội khó khăn, đặc biệt khó khăn theo quy định của pháp luật, thông qua ưu tiên bố trí nguồn lực từ ngân sách nhà nước và huy động nguồn lực xã hội hóa quy định tại khoản 1, khoản 3 Điều này, bảo đảm mức độ an ninh dữ liệu tương xứng trên phạm vi cả nước, không tạo khoảng cách rủi ro giữa các địa bàn.

6. Chính phủ quy định chi tiết cơ chế tiếp nhận thông tin, khen thưởng, quy trình và phạm vi bảo vệ người thông báo quy định tại khoản 2 Điều này; tiêu chí xác định địa bàn và mức hỗ trợ đầu tư hạ tầng quy định tại khoản 5 Điều

này; trường hợp xây dựng khung sản phẩm bảo hiểm rủi ro an ninh dữ liệu đặc thù theo khoản 4 Điều này, điều kiện bảo hiểm được quy định tại văn bản quy phạm pháp luật riêng theo đề xuất của Bộ Tài chính.

Điều 23. Quản lý nhà nước về an ninh dữ liệu; thanh tra, kiểm tra và xử lý vi phạm

1. Chính phủ thống nhất quản lý nhà nước về an ninh dữ liệu trên phạm vi toàn quốc, bao gồm: xây dựng, ban hành chiến lược, chính sách, văn bản quy phạm pháp luật; thiết lập, quản lý hệ thống cấp độ rủi ro an ninh dữ liệu, hệ thống tiêu chuẩn, quy chuẩn kỹ thuật; quản lý hạ tầng giám sát an ninh dữ liệu tập trung, cơ chế thử nghiệm có kiểm soát và hoạt động chứng nhận hợp quy; tổ chức thanh tra, kiểm tra, xử lý vi phạm và điều phối hợp tác quốc tế.

2. Trong phạm vi được Luật này giao quy định chi tiết, Chính phủ quy định nội dung có tính nguyên tắc, khung, gồm ngưỡng định lượng, thời hạn thực hiện, yêu cầu chung về an ninh và tiêu chuẩn, quy chuẩn kỹ thuật khung; việc xây dựng, thẩm định, công bố tiêu chuẩn quốc gia và ban hành quy chuẩn kỹ thuật quốc gia cụ thể về an ninh dữ liệu thuộc thẩm quyền của Bộ trưởng Bộ Công an, Bộ trưởng Bộ Quốc phòng theo lĩnh vực quản lý, thực hiện theo quy định của pháp luật về tiêu chuẩn và quy chuẩn kỹ thuật.

3. Bộ Công an chịu trách nhiệm trước Chính phủ, là cơ quan chủ trì, điều phối tổng thể: tham mưu ban hành chính sách, pháp luật; chủ trì điều phối ứng phó tình huống khẩn cấp; giao lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an thực hiện chức năng Trung tâm Quản trị an ninh dữ liệu quốc gia quy định tại khoản 14 Điều 2 của Luật này và vận hành Hệ thống giám sát an ninh dữ liệu tập trung quốc gia, không thành lập đơn vị mới; chủ trì thẩm định an ninh dữ liệu đối với hoạt động đầu tư, chuyển giao công nghệ, chuyển dữ liệu Cấp độ 4 ra nước ngoài và tiếp nhận thông báo, giám sát việc chuyển dữ liệu Cấp độ 3 ra nước ngoài theo quy định tại Điều 17 của Luật này; thanh tra, kiểm tra, xử lý vi phạm pháp luật về an ninh dữ liệu. Chủ trì, nghiên cứu, thẩm định các giải pháp mật mã bảo đảm an ninh dữ liệu.

4. Bộ Quốc phòng thực hiện chức năng quản lý nhà nước, chịu trách nhiệm toàn diện trước Chính phủ về an ninh dữ liệu trong lĩnh vực quân sự, quốc phòng; tự chủ trì tổ chức thẩm định, kiểm tra, đánh giá rủi ro, kiểm toán, giám sát và ứng phó sự cố đối với dữ liệu thuộc phạm vi quản lý. Đối với cơ quan, đơn vị, doanh nghiệp thuộc phạm vi quản lý của Bộ Quốc phòng có hoạt động dân sự, kinh tế thì trách nhiệm bảo vệ an ninh dữ liệu thực hiện theo quy định chung của Luật này. Chủ trì nghiên cứu, thẩm định các giải pháp mật mã bảo đảm an ninh dữ liệu quân sự.

5. Bộ Khoa học và Công nghệ quản lý nhà nước về khoa học, công nghệ, tiêu chuẩn, quy chuẩn kỹ thuật trong bảo vệ an ninh dữ liệu. Ban Cơ yếu Chính

phủ quản lý nhà nước về cơ yếu, chủ trì nghiên cứu, thẩm định các giải pháp, kỹ thuật mật mã cơ yếu.

6. Người đứng đầu cơ quan, tổ chức, địa phương chịu trách nhiệm trực tiếp về an ninh dữ liệu trong phạm vi quản lý; tổ chức xác định cấp độ rủi ro an ninh dữ liệu, báo cáo theo thủ tục thống nhất tại Điều 20 của Luật này; bố trí nguồn lực, kinh phí, ưu tiên mua sắm, sử dụng sản phẩm công nghệ bảo mật nội địa đã chứng nhận hợp quy; chấp hành mệnh lệnh điều phối kỹ thuật khẩn cấp, tạo điều kiện cho hoạt động thanh tra, kiểm tra.

7. Thủ tục hành chính về an ninh dữ liệu quy định tại Luật này được tổ chức thống nhất thành 02 nhóm thủ tục, do Bộ Công an là đầu mối tiếp nhận:

a) Nhóm thẩm định, đánh giá, chứng nhận, chấp thuận trước khi hệ thống, sản phẩm, dịch vụ, nhân sự, công nghệ mới được đưa vào vận hành, lưu thông, thử nghiệm hoặc trước khi chuyển dữ liệu Cấp độ 4 ra nước ngoài, quy định tại khoản 3, khoản 5 Điều 10, Điều 14, Điều 17 khoản 2 đối với dữ liệu Cấp độ 4, Điều 21 khoản 3, khoản 4 của Luật này;

b) Nhóm thông báo, báo cáo, khai báo an ninh dữ liệu trong quá trình vận hành và khi chuyển dữ liệu Cấp độ 3 ra nước ngoài, quy định tại Điều 8 khoản 5, Điều 17 khoản 2 đối với dữ liệu Cấp độ 3, Điều 20 khoản 2, khoản 4 của Luật này.

Đối với từng thủ tục thuộc hai nhóm quy định tại khoản này, Chính phủ quy định cụ thể chủ thể phải thực hiện, cơ quan giải quyết, thành phần hồ sơ, thời hạn giải quyết, kết quả thủ tục và cơ chế sử dụng lại thông tin, hồ sơ, kết quả đã có, không yêu cầu tổ chức, cá nhân cung cấp lại nhiều lần cho cùng một nội dung.

8. Thanh tra Bộ Công an, Thanh tra Bộ Quốc phòng, Thanh tra Cơ yếu trong phạm vi chức năng, nhiệm vụ theo pháp luật về thanh tra, chủ trì, phối hợp thực hiện thanh tra về an ninh dữ liệu. Không tổ chức thanh tra, kiểm tra về an ninh dữ liệu quá 01 lần trong 01 năm đối với cùng một đối tượng, trừ trường hợp có dấu hiệu vi phạm rõ ràng hoặc theo yêu cầu phục vụ công tác quản lý nhà nước đột xuất; kết quả kiểm toán an ninh dữ liệu độc lập do tổ chức đánh giá sự phù hợp được công nhận thực hiện được xem xét sử dụng làm căn cứ, giảm nội dung, tần suất thanh tra, kiểm tra trực tiếp tương ứng.

9. Chế tài quy định tại khoản này là xử phạt vi phạm hành chính, không thay thế trách nhiệm hình sự; hành vi có đủ yếu tố cấu thành tội phạm thì bị truy cứu trách nhiệm hình sự theo quy định của Bộ luật Hình sự. Tổ chức, cá nhân vi phạm quy định của Luật này thì tùy tính chất, mức độ bị xử lý kỷ luật, xử phạt vi phạm hành chính hoặc truy cứu trách nhiệm hình sự; gây thiệt hại phải bồi thường. Hành vi vi phạm hành chính nghiêm trọng trong lĩnh vực an ninh dữ liệu là hành vi cố ý hoặc buông lỏng quản lý gây rò rỉ, chiếm đoạt, phá hoại dữ

liệu Cấp độ 3, dữ liệu Cấp độ 4, gây hậu quả đặc biệt nghiêm trọng đến quốc phòng, an ninh quốc gia, lợi ích công cộng, theo tiêu chí do Chính phủ quy định. Tổ chức vi phạm hành chính nghiêm trọng bị phạt tiền theo tỷ lệ phần trăm doanh thu năm tài chính liền kề trước đó, mức tối đa không quá 5% doanh thu tại Việt Nam; đối với tập đoàn đa quốc gia, nếu doanh thu tại Việt Nam thấp hơn 5% doanh thu hợp nhất toàn cầu hoặc hậu quả vi phạm vượt phạm vi lãnh thổ Việt Nam thì áp dụng mức tối đa không quá 5% doanh thu toàn cầu của tập đoàn; trường hợp không đủ dữ liệu doanh thu thì áp dụng mức phạt tiền tuyệt đối tối đa theo khung do Chính phủ quy định. Phương pháp xác định doanh thu, năm tài chính thực hiện theo pháp luật về thuế thu nhập doanh nghiệp; Chính phủ quy định chi tiết trình tự áp dụng mức phạt theo doanh thu quy định tại khoản này. Thẩm quyền xử phạt và nguyên tắc xử lý hành vi giao thoa với pháp luật về an ninh mạng, bảo vệ dữ liệu cá nhân thực hiện theo khoản 10 Điều này và pháp luật về xử lý vi phạm hành chính.

10. Một hành vi vi phạm đồng thời cấu thành vi phạm quy định của Luật này và pháp luật về an ninh mạng hoặc pháp luật về bảo vệ dữ liệu cá nhân thì chỉ bị xử phạt một lần theo khung phạt cao hơn. Đối với sự cố an ninh dữ liệu phát sinh do bị tấn công mạng ngoài ý muốn mà tổ chức đã áp dụng đầy đủ, kịp thời các biện pháp bảo vệ an ninh dữ liệu theo quy định của Luật này và không có lỗi thì không bị xử phạt vi phạm hành chính đối với sự cố đó; trường hợp tổ chức đã được cơ quan có thẩm quyền cảnh báo bằng văn bản về nguy cơ, lỗ hổng cụ thể mà không thực hiện biện pháp khắc phục dẫn đến sự cố thì bị xem xét xử lý theo mức độ lỗi tương ứng.

11. Chính phủ quy định chi tiết nội dung quản lý nhà nước, trách nhiệm của các Bộ, cơ quan ngang Bộ, Ủy ban nhân dân các cấp; phương thức, trình tự thanh tra, kiểm tra; hành vi vi phạm, hình thức, mức xử phạt cụ thể và chính sách khoan hồng đối với doanh nghiệp nhỏ, doanh nghiệp khởi nghiệp sáng tạo chủ động khắc phục hậu quả sự cố.

CHƯƠNG VI
ĐIỀU KHOẢN THI HÀNH

Điều 24. Sửa đổi, bổ sung, bãi bỏ quy định của các luật có liên quan

1. Bãi bỏ Điều 26 và khoản 3 Điều 2 Luật An ninh mạng số 116/2025/QH15 kể từ ngày Luật này có hiệu lực thi hành; nội dung giải thích từ ngữ "an ninh dữ liệu" và nội dung bảo đảm an ninh dữ liệu tương ứng tại các quy định bị bãi bỏ thực hiện thống nhất theo quy định tại khoản 2 Điều 2 và Chương II của Luật này. bảo đảm không phát sinh khoảng trống hoặc chồng chéo pháp luật.

2. Sửa đổi, bổ sung khoản 2 Điều 23 Luật Dữ liệu số 60/2024/QH15 theo hướng: việc bảo đảm an ninh dữ liệu khi chuyển, xử lý dữ liệu cốt lõi, dữ liệu quan trọng ra nước ngoài thực hiện theo quy định tại Điều 17 của Luật này; các nội dung khác về điều kiện, trình tự, thủ tục chuyển, xử lý dữ liệu xuyên biên giới tiếp tục thực hiện theo quy định của Luật Dữ liệu số 60/2024/QH15 và văn bản quy định chi tiết.

3. Sửa đổi, bổ sung Điều 20, Điều 21, Điều 22 Luật Bảo vệ dữ liệu cá nhân số 91/2025/QH15 theo hướng: trường hợp dữ liệu chuyển ra nước ngoài hoặc được đánh giá tác động đồng thời là dữ liệu cá nhân và là dữ liệu Cấp độ 3, dữ liệu Cấp độ 4 theo Luật này thì tổ chức thực hiện một thủ tục, lập một hồ sơ duy nhất theo khoản 3 Điều 10, Điều 17 của Luật này, tích hợp đầy đủ nội dung bảo vệ quyền của chủ thể dữ liệu cá nhân theo Luật Bảo vệ dữ liệu cá nhân số 91/2025/QH15.

4. Sửa đổi, bổ sung quy định về mật mã dân sự tại pháp luật về cơ yếu theo hướng: phạm vi mật mã dân sự không bao gồm giải pháp mật mã an ninh do Bộ Công an nghiên cứu, phát triển, công bố, kiểm định phục vụ bảo đảm an ninh mạng, an ninh dữ liệu quy định tại khoản 16 Điều 2 và khoản 4 Điều 6 của Luật này.

5. Sửa đổi, bổ sung Luật Xử lý vi phạm hành chính để bổ sung hình thức, thẩm quyền áp dụng mức phạt tiền theo tỷ lệ doanh thu quy định tại khoản 9 Điều 23 của Luật này là chế tài đặc thù áp dụng riêng cho lĩnh vực an ninh dữ liệu, không thay thế khung phạt tiền tuyệt đối hiện hành áp dụng cho lĩnh vực an ninh mạng, dữ liệu.

Điều 25. Hiệu lực thi hành, điều khoản chuyển tiếp và quy định chi tiết thi hành

1. Luật này có hiệu lực thi hành từ ngày … tháng … năm 2027.

2. Hồ sơ, giấy phép, chứng nhận, văn bản chấp thuận về an ninh mạng, an ninh dữ liệu đã được lập, cấp hoặc tiếp nhận trước ngày Luật này có hiệu lực tiếp tục có giá trị đến hết thời hạn ghi trên văn bản; khi cập nhật, gia hạn hoặc lập mới thì thực hiện theo quy định của Luật này.

3. Cơ quan, tổ chức, cá nhân đang xử lý dữ liệu Cấp độ 3, dữ liệu Cấp độ 4 có trách nhiệm hoàn thành kiểm kê, xác định dữ liệu đang xử lý thuộc Danh mục dữ liệu quan trọng, dữ liệu cốt lõi, đăng ký và nâng cấp biện pháp bảo vệ theo cấp độ trong thời hạn chuyển tiếp, tối đa không quá 36 tháng kể từ ngày Luật này có hiệu lực; Chính phủ quy định thời hạn cụ thể cho từng nhóm nghĩa vụ và từng nhóm đối tượng trong phạm vi thời hạn tối đa nêu trên, trong đó tổ chức, hệ thống thuộc lĩnh vực trọng yếu có quy mô nhỏ hơn được áp dụng thời hạn dài hơn tương ứng. Việc kiểm kê, đăng ký theo khoản này không phải là thủ

tục xác nhận lại cấp độ rủi ro đối với dữ liệu đã thuộc Danh mục dữ liệu quan trọng, dữ liệu cốt lõi.

4. Hệ thống thông tin đang vận hành, dữ liệu đã được xác định cấp độ rủi ro an ninh, hồ sơ đánh giá tác động đã lập, hợp đồng chuyển dữ liệu xuyên biên giới đã ký, sản phẩm, dịch vụ đã được chứng nhận hợp quy, nhân sự, chuyên gia đang làm việc trước ngày Luật này có hiệu lực tiếp tục được sử dụng và hoàn thiện theo quy định của Luật này trong thời hạn chuyển tiếp, bảo đảm không gián đoạn hoạt động.

5. Chính phủ rà soát, trình cấp có thẩm quyền sửa đổi, bổ sung, bãi bỏ hoặc ban hành theo thẩm quyền các nghị định, văn bản hướng dẫn thi hành có liên quan, bảo đảm đồng bộ, không tạo khoảng trống pháp lý và không chồng chéo trong áp dụng thực hiện, đặc biệt đối với văn bản hướng dẫn Luật An ninh mạng số 116/2025/QH15 chịu tác động trực tiếp bởi việc bãi bỏ quy định tại khoản 1 Điều 24 của Luật này.

6. Chính phủ quy định chi tiết thời hạn chuyển tiếp cho từng nhóm nghĩa vụ và từng nhóm đối tượng quy định tại khoản 3 Điều này, bao gồm đánh giá tác động, thẩm định, kết nối giám sát, chuyển dữ liệu xuyên biên giới, chứng nhận sản phẩm và nhân sự; lộ trình kết nối Hệ thống giám sát an ninh dữ liệu tập trung quốc gia và thời hạn lưu trữ nhật ký đối với hệ thống, hồ sơ, sản phẩm, nhân sự quy định tại khoản 4 Điều này.

7. Chính phủ quy định chi tiết các điều, khoản được giao trong Luật và hướng dẫn thi hành các nội dung cần thiết khác để bảo đảm thi hành thống nhất Luật này.