

Số: /2026/QĐ-UBND

Gia Lai, ngày tháng năm 2026

DỰ THẢO

QUYẾT ĐỊNH

Ban hành Quy chế Bảo vệ dữ liệu cá nhân trong hoạt động của các cơ quan nhà nước trên địa bàn tỉnh Gia Lai

Căn cứ Luật Tổ chức chính quyền địa phương số 72/2025/QH15;

Căn cứ Luật Ban hành văn bản quy phạm pháp luật số 64/2025/QH15 được sửa đổi, bổ sung bởi Luật số 87/2025/QH15;

Căn cứ Luật An ninh mạng số 116/2025/QH15;

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

Căn cứ Luật Dữ liệu số 60/2024/QH15;

Căn cứ Nghị định số 356/2025/NĐ-CP, ngày 31/12/2025 của Chính phủ quy định chi tiết một số điều và biện pháp thi hành Luật Bảo vệ dữ liệu cá nhân;

Căn cứ Nghị định số 165/2025/NĐ-CP, ngày 30/6/2025 của Chính phủ quy định chi tiết một số điều và biện pháp thi hành Luật Dữ liệu;

Theo đề nghị của Giám đốc Công an tỉnh Gia Lai;

Ủy ban nhân dân ban hành Quy chế bảo vệ dữ liệu cá nhân trong hoạt động của cơ quan nhà nước trên địa bàn tỉnh Gia Lai.

Điều 1. Ban hành kèm theo Quyết định này “Quy chế Bảo vệ dữ liệu cá nhân trong hoạt động của các cơ quan nhà nước trên địa bàn tỉnh Gia Lai”.

Điều 2. Quyết định này có hiệu lực từ ngày tháng năm 2026.

Điều 3. Chánh Văn phòng Ủy ban nhân dân tỉnh, Giám đốc Công an tỉnh, Thủ trưởng các sở, ban, ngành của tỉnh; Chủ tịch Ủy ban nhân dân cấp xã; Thủ trưởng các cơ quan, đơn vị, tổ chức và cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:

- Như Điều 3;
- Văn phòng Chính phủ (để b/c);
- Thường trực Tỉnh ủy, HĐND tỉnh (để b/c);
- Cục A05 - Bộ Công an;
- Cục Kiểm tra văn bản và Tổ chức thi hành pháp luật – Bộ Tư pháp;
- Vụ Pháp chế - Bộ Nội vụ;
- Đoàn Đại biểu Quốc hội tỉnh;
- UBMTTQVN tỉnh và các tổ chức thành viên;
- CT, PCT UBND tỉnh;
- Báo và Phát thanh, Truyền hình Gia Lai;
- Lưu: VT, CAT.

**TM. ỦY BAN NHÂN DÂN
CHỦ TỊCH**

**ỦY BAN NHÂN DÂN
TỈNH GIA LAI**

**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc**

DỰ THẢO

QUY CHẾ

Bảo vệ dữ liệu cá nhân trong hoạt động của các cơ quan nhà nước trên địa bàn tỉnh Gia Lai

(Ban hành kèm theo Quyết định số .../2026/QĐ-UBND)

Chương I

QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh

1. Quy chế này quy định nguyên tắc, yêu cầu, biện pháp và trách nhiệm của các cơ quan, đơn vị trong việc quản lý, xử lý và bảo vệ dữ liệu cá nhân trong phạm vi quản lý của Ủy ban nhân dân tỉnh Gia Lai.

2. Nội dung bảo vệ dữ liệu cá nhân quy định tại Quy chế này được thực hiện trong toàn bộ quá trình xử lý dữ liệu cá nhân, bao gồm thu thập, ghi nhận, phân tích, xác nhận, lưu trữ, chỉnh sửa, cập nhật, khai thác, sử dụng, cung cấp, chia sẻ, truyền đưa, chuyển giao, xóa, hủy và các hoạt động xử lý khác theo quy định của pháp luật.

3. Đối với hoạt động xử lý dữ liệu cá nhân thuộc lĩnh vực đã được pháp luật chuyên ngành quy định cụ thể thì thực hiện theo quy định của pháp luật chuyên ngành; trường hợp pháp luật chuyên ngành không quy định thì thực hiện theo Luật Bảo vệ dữ liệu cá nhân, Nghị định số 356/2025/NĐ-CP và Quy chế này.

Điều 2. Đối tượng áp dụng

1. Các cơ quan chuyên môn, cơ quan hành chính thuộc Ủy ban nhân dân tỉnh; các đơn vị trực thuộc; đơn vị sự nghiệp công lập thuộc phạm vi quản lý của Ủy ban nhân dân tỉnh; Ủy ban nhân dân cấp xã và các cơ quan, đơn vị khác thuộc phạm vi quản lý của Ủy ban nhân dân tỉnh có hoạt động xử lý dữ liệu cá nhân.

2. Cán bộ, công chức, viên chức, người lao động và cá nhân khác có liên quan đến hoạt động xử lý dữ liệu cá nhân tại các cơ quan, đơn vị quy định tại khoản 1 Điều này.

3. Tổ chức, doanh nghiệp, nhà thầu, đơn vị cung cấp dịch vụ và các tổ chức, cá nhân khác có tham gia xử lý dữ liệu cá nhân cho cơ quan, đơn vị quy định tại khoản 1 Điều này thực hiện các nội dung có liên quan theo hợp đồng, thỏa thuận và quy định của pháp luật về bảo vệ dữ liệu cá nhân.

Điều 3. Giải thích từ ngữ

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

1. Dữ liệu cá nhân là dữ liệu số hoặc thông tin dưới dạng khác xác định hoặc giúp xác định một con người cụ thể theo quy định của pháp luật về bảo vệ dữ liệu cá nhân.

2. Xử lý dữ liệu cá nhân là một hoặc nhiều hoạt động tác động tới dữ liệu cá nhân theo quy định của pháp luật về bảo vệ dữ liệu cá nhân.

3. Bên kiểm soát dữ liệu cá nhân là tổ chức, cá nhân quyết định mục đích và phương tiện xử lý dữ liệu cá nhân theo quy định của pháp luật.

4. Bên xử lý dữ liệu cá nhân là tổ chức, cá nhân thực hiện xử lý dữ liệu cá nhân thay mặt cho bên kiểm soát dữ liệu cá nhân thông qua hợp đồng hoặc thỏa thuận với bên kiểm soát dữ liệu cá nhân.

5. Bên kiểm soát và xử lý dữ liệu cá nhân là tổ chức, cá nhân đồng thời quyết định mục đích, phương tiện và trực tiếp thực hiện việc xử lý dữ liệu cá nhân theo quy định của pháp luật.

6. Bảo vệ dữ liệu cá nhân là việc áp dụng các biện pháp quản lý, pháp lý, tổ chức và kỹ thuật nhằm bảo đảm dữ liệu cá nhân được xử lý đúng quy định của pháp luật, đúng mục đích, trong phạm vi cần thiết và được bảo vệ trong suốt quá trình xử lý.

7. Sự cố vi phạm quy định về bảo vệ dữ liệu cá nhân là sự kiện xảy ra trong quá trình xử lý dữ liệu cá nhân dẫn đến dữ liệu cá nhân bị truy cập, sử dụng, tiết lộ, thay đổi, mất, hủy hoặc xử lý trái quy định của pháp luật.

8. Các từ ngữ khác được sử dụng trong Quy chế này được hiểu theo quy định của Luật Bảo vệ dữ liệu cá nhân, Nghị định số 356/2025/NĐ-CP và các văn bản pháp luật có liên quan.

Điều 4. Nguyên tắc bảo vệ dữ liệu cá nhân

1. Việc xử lý dữ liệu cá nhân phải tuân thủ các nguyên tắc quy định tại Luật Bảo vệ dữ liệu cá nhân, Nghị định số 356/2025/NĐ-CP và các quy định pháp luật có liên quan.

2. Cơ quan, đơn vị chỉ xử lý dữ liệu cá nhân trong phạm vi chức năng, nhiệm vụ, quyền hạn được giao và trên cơ sở pháp lý phù hợp với từng hoạt động xử lý dữ liệu cá nhân.

3. Dữ liệu cá nhân được thu thập, xử lý phải phù hợp với mục đích xử lý; bảo đảm tính cần thiết, chính xác và trong phạm vi dữ liệu cần thiết để thực hiện nhiệm vụ theo quy định của pháp luật.

4. Cơ quan, đơn vị phải áp dụng biện pháp quản lý, tổ chức và kỹ thuật phù hợp để bảo vệ dữ liệu cá nhân trong suốt quá trình xử lý, tương ứng với tính chất, mức độ nhạy cảm của dữ liệu và mức độ rủi ro đối với dữ liệu cá nhân.

5. Việc cung cấp, chia sẻ, chuyển giao dữ liệu cá nhân phải có căn cứ pháp lý, đúng mục đích, đúng phạm vi và bảo đảm các yêu cầu về bảo vệ dữ liệu cá nhân theo quy định của pháp luật.

6. Cơ quan, đơn vị, cá nhân tham gia xử lý dữ liệu cá nhân có trách nhiệm chủ động phòng ngừa, phát hiện, ngăn chặn và kịp thời báo cáo, xử lý các hành vi vi phạm quy định về bảo vệ dữ liệu cá nhân theo thẩm quyền.

Điều 5. Xác định và phân loại dữ liệu cá nhân

1. Cơ quan, đơn vị có hoạt động xử lý dữ liệu cá nhân có trách nhiệm rà soát, xác định và lập danh mục dữ liệu cá nhân thuộc phạm vi quản lý, xử lý của mình theo quy định của pháp luật.

2. Dữ liệu cá nhân được phân loại thành dữ liệu cá nhân cơ bản và dữ liệu cá nhân nhạy cảm theo quy định của Luật Bảo vệ dữ liệu cá nhân và Nghị định số 356/2025/NĐ-CP.

3. Căn cứ tính chất, mức độ nhạy cảm, phạm vi, mục đích và mức độ rủi ro trong quá trình xử lý, cơ quan, đơn vị xác định biện pháp bảo vệ phù hợp đối với từng loại dữ liệu cá nhân.

4. Việc xử lý dữ liệu cá nhân nhạy cảm phải thực hiện các biện pháp bảo vệ theo quy định của pháp luật, bảo đảm kiểm soát chặt chẽ việc truy cập, khai thác, sử dụng, cung cấp và chia sẻ dữ liệu.

5. Cơ quan, đơn vị có trách nhiệm thường xuyên rà soát, cập nhật danh mục dữ liệu cá nhân và biện pháp bảo vệ khi có thay đổi về mục đích, phạm vi, hệ thống, phương thức hoặc hoạt động xử lý dữ liệu cá nhân.

Điều 6. Xác định vai trò trong hoạt động xử lý dữ liệu cá nhân

1. Căn cứ mục đích, phương thức và tính chất của hoạt động xử lý dữ liệu cá nhân, cơ quan, đơn vị xác định vai trò là bên kiểm soát dữ liệu cá nhân, bên xử lý dữ liệu cá nhân hoặc bên kiểm soát và xử lý dữ liệu cá nhân theo quy định của pháp luật.

2. Việc xác định vai trò quy định tại khoản 1 Điều này phải phù hợp với chức năng, nhiệm vụ, quyền hạn của cơ quan, đơn vị và bản chất thực tế của hoạt động xử lý dữ liệu cá nhân; không chỉ căn cứ vào tên gọi của hợp đồng, thỏa thuận hoặc hệ thống thông tin.

3. Trường hợp cơ quan, đơn vị thuê, giao hoặc sử dụng dịch vụ của tổ chức, cá nhân khác để xử lý dữ liệu cá nhân thì phải xác định rõ trách nhiệm của các bên trong việc bảo vệ dữ liệu cá nhân và thực hiện các yêu cầu theo quy định của pháp luật.

4. Việc xác định vai trò của các bên trong hoạt động xử lý dữ liệu cá nhân phải được thể hiện trong hồ sơ, hợp đồng, thỏa thuận hoặc tài liệu có liên quan theo quy định của pháp luật và phù hợp với thực tế xử lý dữ liệu.

Chương II

QUẢN LÝ VÀ XỬ LÝ DỮ LIỆU CÁ NHÂN

Điều 7. Xác định mục đích và phạm vi xử lý dữ liệu cá nhân

1. Trước khi thực hiện hoạt động xử lý dữ liệu cá nhân, cơ quan, đơn vị phải xác định rõ mục đích, phạm vi, loại dữ liệu cá nhân cần xử lý, đối tượng dữ liệu, phương thức xử lý và thời gian xử lý phù hợp với chức năng, nhiệm vụ, quyền hạn được giao và quy định của pháp luật.

2. Việc thu thập, xử lý dữ liệu cá nhân phải bảo đảm dữ liệu được xử lý đúng mục đích, trong phạm vi cần thiết và phù hợp với cơ sở pháp lý của hoạt động xử lý.

3. Cơ quan, đơn vị không thu thập, yêu cầu cung cấp hoặc xử lý dữ liệu cá nhân vượt quá phạm vi cần thiết để thực hiện nhiệm vụ, giải quyết công việc hoặc cung cấp dịch vụ theo quy định của pháp luật.

4. Khi mục đích hoặc phạm vi xử lý dữ liệu cá nhân thay đổi, cơ quan, đơn vị phải rà soát, xác định lại cơ sở pháp lý, phạm vi, loại dữ liệu và biện pháp bảo vệ trước khi thực hiện việc xử lý theo mục đích mới.

Điều 8. Xử lý dữ liệu cá nhân không cần sự đồng ý của chủ thể dữ liệu cá nhân

1. Việc xử lý dữ liệu cá nhân không cần sự đồng ý của chủ thể dữ liệu cá nhân chỉ được thực hiện trong các trường hợp quy định tại Điều 19 Luật Bảo vệ dữ liệu cá nhân và các trường hợp khác theo quy định của pháp luật.

2. Đối với trường hợp xử lý dữ liệu cá nhân để phục vụ hoạt động của cơ quan nhà nước, hoạt động quản lý nhà nước theo quy định của pháp luật, cơ quan, đơn vị phải bảo đảm:

- a) Hoạt động xử lý thuộc chức năng, nhiệm vụ, quyền hạn được giao;
- b) Xác định rõ mục đích và phạm vi xử lý;
- c) Chỉ xử lý loại dữ liệu cá nhân cần thiết cho việc thực hiện nhiệm vụ;
- d) Áp dụng biện pháp bảo vệ dữ liệu cá nhân phù hợp với tính chất, mức độ nhạy cảm của dữ liệu và mức độ rủi ro trong quá trình xử lý.

3. Cơ quan, đơn vị thực hiện xử lý dữ liệu cá nhân không cần sự đồng ý của chủ thể dữ liệu phải thiết lập cơ chế giám sát, trong đó xác định trách nhiệm của cơ quan, đơn vị, bộ phận và cá nhân có liên quan; áp dụng biện pháp bảo vệ phù hợp; kiểm tra, đánh giá việc tuân thủ và tiếp nhận, xử lý phản ánh, kiến nghị theo quy định của pháp luật.

4. Việc xử lý dữ liệu cá nhân trong các trường hợp quy định tại Điều này không làm mất hoặc hạn chế các quyền của chủ thể dữ liệu cá nhân theo quy định của pháp luật, trừ trường hợp pháp luật có quy định khác.

Điều 9. Thực hiện quyền của chủ thể dữ liệu cá nhân

1. Cơ quan, đơn vị có hoạt động xử lý dữ liệu cá nhân có trách nhiệm xây dựng hoặc áp dụng quy trình, thủ tục và biểu mẫu phù hợp để tiếp nhận, xem xét và thực hiện quyền của chủ thể dữ liệu cá nhân theo quy định của pháp luật.

2. Quy trình thực hiện quyền của chủ thể dữ liệu cá nhân phải xác định rõ:

- a) Đầu mối tiếp nhận và xử lý yêu cầu;
- b) Phương thức tiếp nhận và xác minh yêu cầu;
- c) Trách nhiệm của các bộ phận, cá nhân có liên quan;
- d) Trình tự xử lý, thời hạn giải quyết và phương thức phản hồi;
- đ) Việc lưu trữ hồ sơ, tài liệu liên quan đến quá trình tiếp nhận và giải quyết yêu cầu.

3. Khi nhận được yêu cầu của chủ thể dữ liệu cá nhân thuộc phạm vi trách nhiệm giải quyết, cơ quan, đơn vị thực hiện việc tiếp nhận, xác minh, xử lý và

phản hồi theo thời hạn, trình tự, thủ tục quy định tại Luật Bảo vệ dữ liệu cá nhân và Nghị định số 356/2025/NĐ-CP.

4. Trường hợp yêu cầu của chủ thể dữ liệu cá nhân liên quan đến hoạt động xử lý do bên xử lý dữ liệu cá nhân hoặc bên thứ ba thực hiện, cơ quan, đơn vị có trách nhiệm phối hợp với các bên có liên quan để thực hiện quyền của chủ thể dữ liệu theo quy định của pháp luật.

5. Việc thực hiện quyền của chủ thể dữ liệu cá nhân phải bảo đảm không làm ảnh hưởng đến hoạt động của cơ quan nhà nước, quyền và lợi ích hợp pháp của tổ chức, cá nhân khác và các trường hợp hạn chế thực hiện quyền theo quy định của pháp luật.

Điều 10. Thu thập, sử dụng và cập nhật dữ liệu cá nhân

1. Cơ quan, đơn vị chỉ thu thập dữ liệu cá nhân phù hợp với mục đích xử lý đã xác định và cơ sở pháp lý của hoạt động xử lý.

2. Dữ liệu cá nhân được thu thập phải bảo đảm tính chính xác, đầy đủ trong phạm vi cần thiết cho mục đích xử lý; cơ quan, đơn vị có trách nhiệm thực hiện việc cập nhật, điều chỉnh dữ liệu khi phát hiện dữ liệu không chính xác hoặc không còn phù hợp.

3. Việc sử dụng dữ liệu cá nhân phải đúng mục đích, phạm vi và cơ sở pháp lý đã xác định; trường hợp sử dụng dữ liệu cá nhân cho mục đích khác phải xác định cơ sở pháp lý và thực hiện theo quy định của pháp luật.

4. Cơ quan, đơn vị có trách nhiệm kiểm soát việc truy cập, khai thác và sử dụng dữ liệu cá nhân; chỉ cho phép cán bộ, công chức, viên chức, người lao động và cá nhân có liên quan tiếp cận dữ liệu trong phạm vi nhiệm vụ được giao.

5. Không sử dụng dữ liệu cá nhân được cơ quan, đơn vị quản lý cho mục đích cá nhân hoặc mục đích khác không thuộc phạm vi nhiệm vụ, quyền hạn được giao.

Điều 11. Cung cấp, chia sẻ và chuyển giao dữ liệu cá nhân

1. Việc cung cấp, chia sẻ, chuyển giao dữ liệu cá nhân giữa các cơ quan, đơn vị phải có căn cứ pháp lý, đúng mục đích, phạm vi và đối tượng được phép tiếp nhận theo quy định của pháp luật.

2. Trước khi cung cấp, chia sẻ hoặc chuyển giao dữ liệu cá nhân, cơ quan, đơn vị cung cấp dữ liệu có trách nhiệm xác định:

- a) Mục đích và căn cứ cung cấp, chia sẻ hoặc chuyển giao;
- b) Loại dữ liệu cá nhân được cung cấp;
- c) Đối tượng tiếp nhận dữ liệu;
- d) Phương thức và phạm vi cung cấp, chia sẻ hoặc chuyển giao;

đ) Biện pháp bảo vệ dữ liệu cá nhân trong quá trình cung cấp, chia sẻ hoặc chuyển giao.

3. Việc chia sẻ dữ liệu cá nhân giữa các cơ quan, đơn vị thuộc tỉnh được thực hiện thông qua hệ thống, nền tảng, kênh kết nối, chia sẻ dữ liệu được cơ quan có thẩm quyền cho phép và đáp ứng yêu cầu bảo đảm an toàn, bảo mật theo quy định.

4. Không cung cấp, chia sẻ dữ liệu cá nhân cho tổ chức, cá nhân không có căn cứ pháp lý hoặc không có thẩm quyền tiếp nhận dữ liệu.

5. Cơ quan, đơn vị tiếp nhận dữ liệu cá nhân chỉ được sử dụng dữ liệu trong phạm vi, mục đích đã được xác định và có trách nhiệm áp dụng các biện pháp bảo vệ dữ liệu cá nhân theo quy định của pháp luật.

6. Việc chuyển dữ liệu cá nhân xuyên biên giới được thực hiện theo quy định của Luật Bảo vệ dữ liệu cá nhân, Nghị định số 356/2025/NĐ-CP và pháp luật có liên quan.

Điều 12. Xử lý dữ liệu cá nhân thông qua bên xử lý dữ liệu cá nhân

1. Trường hợp cơ quan, đơn vị thuê, giao hoặc sử dụng dịch vụ của tổ chức, cá nhân khác để thực hiện hoạt động xử lý dữ liệu cá nhân, cơ quan, đơn vị phải xác định rõ vai trò, trách nhiệm của các bên theo quy định của pháp luật.

2. Hợp đồng, thỏa thuận hoặc văn bản có liên quan về xử lý dữ liệu cá nhân phải xác định tối thiểu các nội dung sau:

- a) Mục đích, phạm vi và thời gian xử lý dữ liệu cá nhân;
- b) Loại dữ liệu cá nhân được xử lý;
- c) Quyền và trách nhiệm của các bên;
- d) Yêu cầu về bảo mật và bảo vệ dữ liệu cá nhân;
- đ) Biện pháp xử lý, lưu trữ, cung cấp, chia sẻ và xóa, hủy dữ liệu cá nhân;
- e) Trách nhiệm thông báo, phối hợp xử lý khi xảy ra sự cố hoặc vi phạm quy định về bảo vệ dữ liệu cá nhân;
- g) Trách nhiệm chấm dứt xử lý, hoàn trả, xóa hoặc hủy dữ liệu cá nhân khi kết thúc việc cung cấp dịch vụ hoặc theo yêu cầu hợp pháp của cơ quan có thẩm quyền.

3. Cơ quan, đơn vị có trách nhiệm kiểm tra, giám sát việc thực hiện các yêu cầu về bảo vệ dữ liệu cá nhân của bên xử lý dữ liệu cá nhân trong phạm vi trách nhiệm của mình.

4. Bên xử lý dữ liệu cá nhân không được sử dụng dữ liệu cá nhân để thực hiện mục đích riêng hoặc chuyển giao cho bên khác ngoài phạm vi được cơ quan, đơn vị giao, thỏa thuận hoặc pháp luật quy định.

5. Việc sử dụng dịch vụ điện toán đám mây, phần mềm, nền tảng số, hệ thống lưu trữ hoặc dịch vụ công nghệ thông tin có hoạt động xử lý dữ liệu cá nhân phải được đánh giá, kiểm soát các yêu cầu về bảo vệ dữ liệu cá nhân trước và trong quá trình sử dụng.

Điều 13. Lưu trữ, xóa và hủy dữ liệu cá nhân

1. Cơ quan, đơn vị phải xác định thời gian lưu trữ dữ liệu cá nhân phù hợp với mục đích xử lý, yêu cầu nghiệp vụ, quy định của pháp luật chuyên ngành và quy định pháp luật về lưu trữ.

2. Dữ liệu cá nhân phải được lưu trữ bằng biện pháp phù hợp, bảo đảm khả năng kiểm soát truy cập, bảo mật, toàn vẹn và phòng ngừa việc sử dụng, tiết lộ hoặc truy cập trái phép.

3. Khi dữ liệu cá nhân không còn cần thiết cho mục đích xử lý hoặc hết thời hạn lưu trữ theo quy định của pháp luật, cơ quan, đơn vị phải thực hiện việc xóa, hủy hoặc áp dụng biện pháp xử lý phù hợp theo quy định của pháp luật.

4. Việc xóa, hủy dữ liệu cá nhân phải bảo đảm dữ liệu không thể bị khôi phục hoặc tiếp tục sử dụng trái phép, phù hợp với phương thức lưu trữ và yêu cầu kỹ thuật của hệ thống.

5. Trường hợp pháp luật quy định phải tiếp tục lưu trữ dữ liệu cá nhân hoặc dữ liệu cá nhân là thành phần của hồ sơ, tài liệu phải lưu trữ thì việc xóa, hủy dữ liệu được thực hiện theo quy định của pháp luật có liên quan.

6. Cơ quan, đơn vị phải xây dựng hoặc áp dụng quy trình kiểm soát việc xóa, hủy dữ liệu cá nhân, trong đó xác định trách nhiệm, thẩm quyền, phương thức thực hiện và việc ghi nhận kết quả xóa, hủy.

Điều 14. Bảo vệ dữ liệu cá nhân nhạy cảm

1. Cơ quan, đơn vị xử lý dữ liệu cá nhân nhạy cảm phải xác định rõ phạm vi, mục đích, đối tượng được phép truy cập, khai thác và áp dụng biện pháp bảo vệ phù hợp theo quy định của pháp luật.

2. Việc truy cập, khai thác, cung cấp và chia sẻ dữ liệu cá nhân nhạy cảm phải được kiểm soát chặt chẽ; chỉ thực hiện đối với cá nhân, bộ phận có nhiệm vụ và thẩm quyền được giao.

3. Cơ quan, đơn vị phải áp dụng các biện pháp quản lý, tổ chức và kỹ thuật phù hợp để phòng ngừa việc truy cập, sử dụng, sao chép, cung cấp, tiết lộ hoặc xử lý trái phép dữ liệu cá nhân nhạy cảm.

4. Trường hợp dữ liệu cá nhân nhạy cảm được lưu trữ, xử lý trên hệ thống thông tin, cơ quan, đơn vị phải áp dụng biện pháp bảo đảm an toàn hệ thống thông tin, kiểm soát truy cập, xác thực và giám sát phù hợp với tính chất, mức độ rủi ro của dữ liệu.

5. Việc xử lý dữ liệu cá nhân nhạy cảm phải tuân thủ các quy định riêng của pháp luật đối với từng lĩnh vực, loại dữ liệu và hoạt động xử lý.

Điều 15. Bảo vệ dữ liệu cá nhân trên hệ thống thông tin

1. Hệ thống thông tin có hoạt động xử lý dữ liệu cá nhân phải được xác định phạm vi dữ liệu, mục đích xử lý, người sử dụng, quyền truy cập và các biện pháp bảo vệ phù hợp.

2. Việc cấp, thay đổi và thu hồi quyền truy cập dữ liệu cá nhân phải được thực hiện theo nguyên tắc phân quyền phù hợp với chức năng, nhiệm vụ, vị trí công tác và nhu cầu thực tế của người sử dụng.

3. Tài khoản truy cập hệ thống phải được định danh, xác thực và quản lý theo quy định về an toàn hệ thống thông tin, an ninh mạng và quy định nội bộ của cơ quan, đơn vị.

4. Khi cán bộ, công chức, viên chức, người lao động thay đổi vị trí công tác, chuyển đơn vị, nghỉ việc hoặc không còn nhu cầu truy cập, cơ quan, đơn vị phải kịp thời rà soát, điều chỉnh hoặc thu hồi quyền truy cập.

5. Hệ thống thông tin có chức năng xử lý dữ liệu cá nhân phải có khả năng ghi nhận, lưu trữ và bảo vệ nhật ký hoạt động phù hợp với yêu cầu quản lý, kiểm tra, giám sát và quy định pháp luật có liên quan.

6. Cơ quan, đơn vị thực hiện rà soát quyền truy cập và các biện pháp bảo vệ dữ liệu cá nhân định kỳ hoặc khi có thay đổi đáng kể về hệ thống, nhân sự, phương thức hoặc phạm vi xử lý dữ liệu.

7. Không sử dụng dữ liệu cá nhân thật trên môi trường thử nghiệm, phát triển hoặc kiểm thử phần mềm, trừ trường hợp cần thiết và có biện pháp bảo vệ phù hợp theo quy định của pháp luật. Ưu tiên sử dụng dữ liệu giả lập, dữ liệu đã được khử nhận dạng hoặc dữ liệu không chứa thông tin xác định cá nhân.

Điều 16. Bảo vệ dữ liệu cá nhân trong môi trường mạng và ngoài hệ thống thông tin

1. Việc xử lý, lưu trữ, truyền đưa dữ liệu cá nhân ngoài hệ thống thông tin phải được thực hiện bằng phương thức phù hợp, bảo đảm an toàn, bảo mật và đúng phạm vi nhiệm vụ được giao.

2. Khi truyền đưa, sao chép hoặc lưu trữ dữ liệu cá nhân trên thiết bị, phương tiện lưu trữ hoặc qua môi trường mạng, cơ quan, đơn vị phải áp dụng biện pháp bảo vệ phù hợp với tính chất, mức độ nhạy cảm của dữ liệu và mức độ rủi ro.

3. Không sử dụng thư điện tử cá nhân, ứng dụng nhắn tin công cộng, mạng xã hội hoặc các kênh trao đổi không được cơ quan có thẩm quyền cho phép để cung cấp, chia sẻ dữ liệu cá nhân thuộc phạm vi quản lý của cơ quan, đơn vị.

4. Trường hợp cần thiết phải sử dụng phương thức trao đổi dữ liệu khác với hệ thống chính thức của cơ quan, đơn vị, người có thẩm quyền phải xác định phương thức, phạm vi và biện pháp bảo vệ phù hợp trước khi thực hiện.

5. Việc sao chép dữ liệu cá nhân ra khỏi hệ thống, thiết bị hoặc trụ sở cơ quan phải được kiểm soát về thẩm quyền, mục đích, phạm vi dữ liệu và phương thức bảo vệ.

Điều 17. Công khai dữ liệu cá nhân trên môi trường mạng

1. Cơ quan, đơn vị chỉ công khai dữ liệu cá nhân trên cổng thông tin điện tử, trang thông tin điện tử, hệ thống cung cấp dịch vụ công hoặc phương tiện thông tin khác khi có căn cứ pháp lý và phù hợp với mục đích, phạm vi công khai theo quy định của pháp luật.

2. Trước khi đăng tải, công khai thông tin trên môi trường mạng, cơ quan, đơn vị phải rà soát nội dung, hồ sơ, biểu mẫu và dữ liệu kèm theo để hạn chế việc công khai dữ liệu cá nhân không cần thiết hoặc không đúng quy định.

3. Dữ liệu cá nhân nhạy cảm không được công khai trên môi trường mạng nếu không có căn cứ pháp lý cho phép.

4. Cơ quan, đơn vị có trách nhiệm kiểm soát, rà soát và kịp thời gỡ bỏ, điều chỉnh hoặc hạn chế khả năng tiếp cận đối với dữ liệu cá nhân được công khai không đúng quy định.

5. Việc công khai dữ liệu cá nhân phải bảo đảm phù hợp với quy định của pháp luật về bảo vệ dữ liệu cá nhân, tiếp cận thông tin, lưu trữ, bí mật nhà nước và các quy định pháp luật có liên quan.

Chương III

TỔ CHỨC VÀ NHÂN SỰ BẢO VỆ DỮ LIỆU CÁ NHÂN

Điều 18. Chỉ định bộ phận, nhân sự bảo vệ dữ liệu cá nhân

1. Cơ quan, đơn vị có hoạt động xử lý dữ liệu cá nhân có trách nhiệm chỉ định nhân sự bảo vệ dữ liệu cá nhân hoặc bộ phận bảo vệ dữ liệu cá nhân theo quy định của Luật Bảo vệ dữ liệu cá nhân, Nghị định số 356/2025/NĐ-CP và Quy chế này.

2. Việc chỉ định nhân sự hoặc bộ phận bảo vệ dữ liệu cá nhân phải được thực hiện bằng văn bản của người có thẩm quyền của cơ quan, đơn vị; trong đó xác định rõ chức năng, nhiệm vụ, quyền hạn, trách nhiệm và mối quan hệ phối hợp trong công tác bảo vệ dữ liệu cá nhân.

3. Căn cứ quy mô, tính chất, phạm vi và mức độ xử lý dữ liệu cá nhân, cơ cấu tổ chức, vị trí việc làm và điều kiện thực tế, cơ quan, đơn vị quyết định việc:

- a) Chỉ định một hoặc một số nhân sự thực hiện nhiệm vụ bảo vệ dữ liệu cá nhân;
- b) Thành lập hoặc giao nhiệm vụ cho bộ phận bảo vệ dữ liệu cá nhân;
- c) Kết hợp nhân sự hoặc bộ phận bảo vệ dữ liệu cá nhân với chức năng, nhiệm vụ khác phù hợp với quy định của pháp luật.

4. Việc bố trí nhân sự, bộ phận bảo vệ dữ liệu cá nhân phải bảo đảm không làm ảnh hưởng đến việc thực hiện chức năng, nhiệm vụ chuyên môn của cơ quan, đơn vị và phù hợp với vị trí việc làm, điều kiện nhân lực và yêu cầu chuyên môn theo quy định.

5. Trường hợp cơ quan, đơn vị thuê tổ chức, cá nhân cung cấp dịch vụ bảo vệ dữ liệu cá nhân thì việc thuê dịch vụ phải được thực hiện theo quy định của pháp luật và phải xác định rõ phạm vi công việc, trách nhiệm, quyền hạn, yêu cầu bảo mật và trách nhiệm xử lý dữ liệu cá nhân của các bên.

Điều 19. Điều kiện đối với nhân sự bảo vệ dữ liệu cá nhân

1. Nhân sự bảo vệ dữ liệu cá nhân được chỉ định phải đáp ứng các điều kiện theo quy định của pháp luật, bao gồm:

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

2. Trường hợp cơ quan, đơn vị thành lập bộ phận bảo vệ dữ liệu cá nhân, nhân sự thuộc bộ phận phải đáp ứng điều kiện quy định tại khoản 1 Điều này.

3. Cơ quan, đơn vị có trách nhiệm đánh giá, lựa chọn và chỉ định nhân sự bảo vệ dữ liệu cá nhân phù hợp với yêu cầu, quy mô và tính chất hoạt động xử lý dữ liệu cá nhân của mình.

4. Người đứng đầu cơ quan, đơn vị chịu trách nhiệm bảo đảm điều kiện để nhân sự, bộ phận bảo vệ dữ liệu cá nhân thực hiện nhiệm vụ được giao.

5. Cơ quan, đơn vị thực hiện thỏa thuận trách nhiệm bảo mật với nhân sự bảo vệ dữ liệu cá nhân theo quy định của pháp luật.

Điều 20. Nhiệm vụ của bộ phận và nhân sự bảo vệ dữ liệu cá nhân

1. Bộ phận bảo vệ dữ liệu cá nhân có các nhiệm vụ sau:

a) Tham mưu xây dựng, rà soát và tổ chức thực hiện chính sách, quy trình, quy định và biểu mẫu về bảo vệ dữ liệu cá nhân trong cơ quan, đơn vị;

b) Tổ chức hoặc phối hợp tổ chức thực hiện quyền của chủ thể dữ liệu cá nhân theo quy định của pháp luật;

c) Định kỳ đánh giá thực trạng tuân thủ pháp luật về bảo vệ dữ liệu cá nhân; tổng hợp, báo cáo và đề xuất biện pháp nâng cao hiệu quả tuân thủ, phòng ngừa và kiểm soát rủi ro;

d) Thực hiện hoặc phối hợp thực hiện hồ sơ đánh giá tác động xử lý dữ liệu cá nhân, hồ sơ đánh giá tác động chuyển dữ liệu cá nhân xuyên biên giới trong trường hợp pháp luật quy định;

đ) Tiếp nhận, tổng hợp và báo cáo vi phạm quy định về bảo vệ dữ liệu cá nhân; phối hợp ứng phó, khắc phục sự cố theo quy định;

e) Xây dựng hoặc phối hợp xây dựng kế hoạch đào tạo, bồi dưỡng, tuyên truyền, nâng cao nhận thức về bảo vệ dữ liệu cá nhân;

g) Phối hợp triển khai các biện pháp kỹ thuật, biện pháp quản lý và biện pháp tổ chức nhằm bảo vệ dữ liệu cá nhân;

h) Phối hợp xây dựng và triển khai kế hoạch ứng phó, khắc phục sự cố liên quan đến bảo vệ dữ liệu cá nhân;

i) Tham mưu người đứng đầu cơ quan, đơn vị các vấn đề có liên quan đến việc bảo vệ dữ liệu cá nhân theo chức năng, nhiệm vụ được giao.

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

a) Tham mưu xây dựng, rà soát và tổ chức thực hiện chính sách, quy trình, quy định và biểu mẫu về bảo vệ dữ liệu cá nhân;

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

c) Tham gia đánh giá việc tuân thủ pháp luật về bảo vệ dữ liệu cá nhân và đề xuất biện pháp phòng ngừa, kiểm soát rủi ro;

d) Thực hiện hoặc phối hợp thực hiện hồ sơ đánh giá tác động xử lý dữ liệu cá nhân, hồ sơ đánh giá tác động chuyển dữ liệu cá nhân xuyên biên giới và các yêu cầu khác theo quy định của pháp luật;

đ) Tiếp nhận, tổng hợp, báo cáo vi phạm quy định về bảo vệ dữ liệu cá nhân và phối hợp xử lý theo thẩm quyền;

- e) Tham gia các chương trình đào tạo, bồi dưỡng về bảo vệ dữ liệu cá nhân;
- g) Tham gia triển khai các biện pháp kỹ thuật, biện pháp quản lý và kế hoạch ứng phó, khắc phục sự cố bảo vệ dữ liệu cá nhân.

3. Bộ phận, nhân sự bảo vệ dữ liệu cá nhân thực hiện nhiệm vụ theo sự phân công của người đứng đầu cơ quan, đơn vị và chịu trách nhiệm về việc thực hiện nhiệm vụ được giao theo quy định của pháp luật.

Điều 21. Trách nhiệm của cơ quan, đơn vị đối với bộ phận, nhân sự bảo vệ dữ liệu cá nhân

1. Bảo đảm điều kiện cần thiết để bộ phận, nhân sự bảo vệ dữ liệu cá nhân thực hiện nhiệm vụ được giao theo quy định của pháp luật và Quy chế này.

2. Tạo điều kiện cho nhân sự bảo vệ dữ liệu cá nhân được tham gia các chương trình đào tạo, bồi dưỡng, cập nhật kiến thức pháp luật, kỹ năng chuyên môn và các yêu cầu mới về bảo vệ dữ liệu cá nhân.

3. Bảo đảm bộ phận, nhân sự bảo vệ dữ liệu cá nhân được tiếp cận các thông tin, hồ sơ, tài liệu cần thiết trong phạm vi thẩm quyền để thực hiện nhiệm vụ, đồng thời phải tuân thủ các yêu cầu về bảo mật, bí mật nhà nước và các quy định pháp luật có liên quan.

4. Khi có thay đổi về nhân sự, cơ cấu tổ chức hoặc hoạt động xử lý dữ liệu cá nhân làm ảnh hưởng đến việc thực hiện nhiệm vụ bảo vệ dữ liệu cá nhân, cơ quan, đơn vị phải kịp thời rà soát, điều chỉnh việc phân công hoặc chỉ định nhân sự, bộ phận bảo vệ dữ liệu cá nhân.

5. Trường hợp nhân sự hoặc bộ phận bảo vệ dữ liệu cá nhân không còn đáp ứng điều kiện theo quy định hoặc không tiếp tục thực hiện nhiệm vụ, cơ quan, đơn vị phải thực hiện việc thay thế, điều chỉnh hoặc chỉ định lại theo quy định.

6. Việc chỉ định, thay đổi hoặc chấm dứt việc chỉ định nhân sự, bộ phận bảo vệ dữ liệu cá nhân phải được lập thành văn bản và lưu giữ theo quy định.

Chương IV

ỨNG PHÓ SỰ CỐ VÀ THÔNG BÁO VI PHẠM QUY ĐỊNH VỀ BẢO VỆ DỮ LIỆU CÁ NHÂN

Điều 22. Phát hiện, tiếp nhận và báo cáo sự cố vi phạm quy định về bảo vệ dữ liệu cá nhân

1. Khi phát hiện hoặc có căn cứ xác định xảy ra sự cố có nguy cơ làm mất, lộ, lọt, thay đổi, hủy hoại, truy cập, sử dụng, cung cấp hoặc xử lý trái phép dữ liệu cá nhân, cá nhân, bộ phận phát hiện phải kịp thời báo cáo người đứng đầu cơ quan, đơn vị và bộ phận, nhân sự bảo vệ dữ liệu cá nhân.

2. Báo cáo ban đầu phải được thực hiện bằng phương thức phù hợp với tính chất, mức độ khẩn cấp của sự cố; trong trường hợp cần thiết có thể báo cáo ngay bằng phương thức liên lạc nhanh nhất và bổ sung bằng văn bản sau đó.

3. Nội dung báo cáo ban đầu, trong phạm vi thông tin đã xác định, gồm:

- a) Thời gian, địa điểm và phương thức phát hiện sự cố;
- b) Hệ thống thông tin, thiết bị, hồ sơ hoặc phương tiện lưu trữ có liên quan;

- c) Loại dữ liệu cá nhân có khả năng bị ảnh hưởng;
- d) Phạm vi, số lượng dữ liệu cá nhân và chủ thể dữ liệu có khả năng bị ảnh hưởng;
- đ) Nguyên nhân hoặc dấu hiệu nguyên nhân của sự cố, nếu đã xác định;
- e) Biện pháp đã được thực hiện để ngăn chặn, hạn chế và khắc phục sự cố.

4. Trường hợp sự cố liên quan đến hệ thống thông tin, cơ quan, đơn vị phải đồng thời thực hiện quy trình ứng cứu sự cố an toàn thông tin mạng, an ninh mạng và các quy trình chuyên ngành có liên quan.

Điều 23. Ứng phó và xử lý sự cố vi phạm quy định về bảo vệ dữ liệu cá nhân

1. Người đứng đầu cơ quan, đơn vị có trách nhiệm chỉ đạo xử lý kịp thời sự cố theo quy trình ứng phó sự cố của cơ quan, đơn vị và quy định của pháp luật.

2. Việc ứng phó sự cố phải bảo đảm các yêu cầu sau:

a) Kịp thời ngăn chặn, hạn chế việc tiếp tục truy cập, sử dụng, tiết lộ, thay đổi, mất hoặc hủy dữ liệu cá nhân trái phép;

b) Xác định phạm vi, nguyên nhân, tính chất và mức độ ảnh hưởng của sự cố;

c) Bảo vệ, thu thập và lưu giữ thông tin, dữ liệu, nhật ký hệ thống và các dấu vết điện tử có liên quan để phục vụ việc xác minh, xử lý và khắc phục sự cố;

d) Thực hiện biện pháp khắc phục, phục hồi hoạt động xử lý dữ liệu cá nhân an toàn và hạn chế nguy cơ tái diễn;

đ) Đánh giá nguy cơ ảnh hưởng đến quyền và lợi ích hợp pháp của chủ thể dữ liệu cá nhân để xác định trách nhiệm thông báo, báo cáo theo quy định của pháp luật.

3. Trong quá trình xử lý sự cố, cơ quan, đơn vị không được tự ý xóa, sửa đổi hoặc làm mất thông tin, dữ liệu và dấu vết có khả năng phục vụ việc xác minh nguyên nhân, phạm vi và tính chất của sự cố, trừ trường hợp việc xóa, sửa đổi là cần thiết để ngăn chặn nguy cơ tiếp tục xảy ra sự cố và phải được ghi nhận.

4. Trường hợp sự cố vượt quá khả năng xử lý của cơ quan, đơn vị, người đứng đầu cơ quan, đơn vị chủ động đề nghị cơ quan, đơn vị có thẩm quyền hoặc tổ chức, cá nhân có năng lực phối hợp xử lý theo quy định của pháp luật.

5. Việc ứng phó sự cố phải bảo đảm đồng thời yêu cầu bảo vệ dữ liệu cá nhân, an toàn hệ thống thông tin, an ninh mạng, bí mật nhà nước và các yêu cầu bảo đảm an toàn, an ninh khác theo quy định của pháp luật.

Điều 24. Thông báo vi phạm quy định về bảo vệ dữ liệu cá nhân

1. Cơ quan, đơn vị với vai trò là bên kiểm soát dữ liệu cá nhân hoặc bên kiểm soát và xử lý dữ liệu cá nhân khi phát hiện vi phạm quy định về bảo vệ dữ liệu cá nhân thuộc trường hợp quy định tại khoản 1 Điều 23 Luật Bảo vệ dữ liệu cá nhân phải thực hiện thông báo cho cơ quan chuyên trách bảo vệ dữ liệu cá nhân theo đúng thời hạn quy định của pháp luật.

2. Thời hạn thông báo quy định tại khoản 1 Điều này là chậm nhất 72 giờ kể từ khi phát hiện hành vi vi phạm thuộc trường hợp phải thông báo theo quy định của pháp luật.

3. Trường hợp bên xử lý dữ liệu cá nhân phát hiện vi phạm, bên xử lý dữ liệu cá nhân phải thông báo kịp thời cho bên kiểm soát dữ liệu cá nhân hoặc bên kiểm soát và xử lý dữ liệu cá nhân để thực hiện các nghĩa vụ theo quy định của pháp luật.

4. Thông báo vi phạm được thực hiện theo nội dung, hình thức, phương thức và mẫu biểu do pháp luật quy định; trường hợp thuộc phạm vi áp dụng Mẫu số 08 ban hành kèm theo Nghị định số 356/2025/NĐ-CP thì thực hiện theo Mẫu số 08.

5. Nội dung thông báo vi phạm phải bảo đảm đầy đủ thông tin theo quy định của pháp luật, trong đó xác định rõ tính chất vi phạm, loại dữ liệu và số lượng dữ liệu có liên quan, thông tin liên hệ của bộ phận hoặc nhân sự bảo vệ dữ liệu cá nhân, hậu quả, thiệt hại có thể xảy ra và biện pháp đã, đang hoặc dự kiến thực hiện để xử lý, giảm thiểu tác hại.

6. Cơ quan, đơn vị phải lập biên bản xác nhận về việc xảy ra vi phạm quy định về bảo vệ dữ liệu cá nhân và phối hợp với cơ quan chuyên trách bảo vệ dữ liệu cá nhân xử lý vi phạm theo quy định của pháp luật.

Điều 25. Thông báo đối với vi phạm liên quan đến dữ liệu vị trí cá nhân và dữ liệu sinh trắc học

1. Khi xảy ra sự cố vi phạm dữ liệu cá nhân liên quan đến dữ liệu vị trí cá nhân hoặc dữ liệu sinh trắc học, cơ quan, đơn vị thực hiện các nghĩa vụ thông báo, báo cáo, ghi nhận và lưu trữ hồ sơ vi phạm theo quy định tại Điều 29 Nghị định số 356/2025/NĐ-CP và các quy định pháp luật có liên quan.

2. Trường hợp thuộc diện phải thông báo cho chủ thể dữ liệu bị ảnh hưởng, cơ quan, đơn vị thực hiện thông báo trong thời hạn và với nội dung theo quy định của pháp luật.

3. Trường hợp không thể thông báo cho toàn bộ chủ thể dữ liệu bị ảnh hưởng trong thời hạn quy định do lý do kỹ thuật hoặc tình huống khẩn cấp, cơ quan, đơn vị thực hiện các biện pháp thông báo thay thế theo quy định của pháp luật và tiếp tục thông báo cho chủ thể dữ liệu ngay khi điều kiện cho phép.

4. Hồ sơ vi phạm liên quan đến dữ liệu vị trí cá nhân và dữ liệu sinh trắc học được ghi nhận, lưu trữ và cập nhật theo thời hạn quy định tại Nghị định số 356/2025/NĐ-CP.

Điều 26. Khắc phục hậu quả và phòng ngừa sự cố tái diễn

1. Sau khi xử lý sự cố, cơ quan, đơn vị có trách nhiệm tổ chức đánh giá nguyên nhân, phạm vi, mức độ ảnh hưởng và hiệu quả của các biện pháp đã thực hiện; xác định trách nhiệm của các tổ chức, bộ phận và cá nhân có liên quan theo quy định của pháp luật.

2. Cơ quan, đơn vị thực hiện các biện pháp cần thiết để khắc phục hậu quả, phục hồi hoạt động, giảm thiểu nguy cơ ảnh hưởng đến quyền và lợi ích hợp pháp của chủ thể dữ liệu và phòng ngừa sự cố tái diễn.

3. Trường hợp sự cố xuất phát từ điểm yếu về quản lý, quy trình, nhân sự hoặc kỹ thuật, cơ quan, đơn vị phải rà soát, điều chỉnh hoặc bổ sung biện pháp bảo vệ dữ liệu cá nhân phù hợp.

4. Trường hợp sự cố có liên quan đến bên xử lý dữ liệu cá nhân, nhà thầu, nhà cung cấp dịch vụ hoặc tổ chức, cá nhân khác, cơ quan, đơn vị phối hợp xác định nguyên nhân, trách nhiệm và biện pháp khắc phục theo hợp đồng, thỏa thuận và quy định của pháp luật.

5. Việc xử lý trách nhiệm đối với tổ chức, cá nhân có hành vi vi phạm quy định về bảo vệ dữ liệu cá nhân được thực hiện theo tính chất, mức độ vi phạm và quy định của pháp luật có liên quan.

6. Hồ sơ về sự cố, biện pháp xử lý, khắc phục và kết quả đánh giá sau sự cố được lưu trữ theo quy định của pháp luật và quy định nội bộ của cơ quan, đơn vị.

Chương V

TRÁCH NHIỆM CỦA CÁC CƠ QUAN, ĐƠN VỊ

Điều 27. Trách nhiệm của Công an tỉnh

1. Là cơ quan đầu mối giúp Ủy ban nhân dân tỉnh tổ chức triển khai, hướng dẫn và theo dõi công tác bảo vệ dữ liệu cá nhân trên địa bàn tỉnh theo quy định của pháp luật và hướng dẫn của Bộ Công an.

2. Chủ trì, phối hợp với các cơ quan, đơn vị có liên quan:

a) Hướng dẫn thực hiện các quy định của pháp luật về bảo vệ dữ liệu cá nhân và Quy chế này;

b) Tuyên truyền, phổ biến, tập huấn, nâng cao nhận thức và kỹ năng bảo vệ dữ liệu cá nhân;

c) Theo dõi, tổng hợp, đánh giá tình hình thực hiện công tác bảo vệ dữ liệu cá nhân trên địa bàn tỉnh;

d) Kiểm tra việc thực hiện Quy chế theo chức năng, nhiệm vụ và thẩm quyền được giao;

đ) Hướng dẫn, phối hợp xử lý các sự cố, vụ việc vi phạm quy định về bảo vệ dữ liệu cá nhân theo thẩm quyền.

3. Là đầu mối phối hợp với cơ quan chuyên trách bảo vệ dữ liệu cá nhân thuộc Bộ Công an và các cơ quan có liên quan trong việc tiếp nhận thông tin, phối hợp kiểm tra, xử lý vi phạm, ứng phó và khắc phục sự cố theo quy định của pháp luật.

4. Tiếp nhận, tổng hợp thông tin, báo cáo của các cơ quan, đơn vị về tình hình bảo vệ dữ liệu cá nhân; trường hợp phát hiện vụ việc có dấu hiệu vi phạm pháp luật thì thực hiện hoặc đề xuất thực hiện các biện pháp xử lý theo thẩm quyền.

5. Chủ trì tổng hợp, tham mưu Ủy ban nhân dân tỉnh báo cáo cơ quan có thẩm quyền về tình hình, kết quả thực hiện công tác bảo vệ dữ liệu cá nhân trên địa bàn tỉnh theo quy định.

6. Phối hợp với các cơ quan, đơn vị rà soát, đánh giá nguy cơ mất an toàn, lộ, lọt dữ liệu cá nhân trong các hệ thống thông tin thuộc phạm vi quản lý; đề xuất biện pháp phòng ngừa, khắc phục phù hợp.

7. Khi thực hiện kiểm tra, hướng dẫn hoặc phối hợp xử lý vụ việc liên quan đến dữ liệu cá nhân phải bảo đảm không làm ảnh hưởng đến hoạt động bình thường của cơ quan, đơn vị, đồng thời tuân thủ quy định về bí mật nhà nước, an ninh mạng, an toàn thông tin và các quy định pháp luật có liên quan.

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

1. Chủ trì, phối hợp với Công an tỉnh và các cơ quan, đơn vị có liên quan tham mưu, tổ chức triển khai các giải pháp kỹ thuật bảo đảm an toàn hệ thống thông tin, cơ sở dữ liệu và hạ tầng số thuộc phạm vi quản lý của tỉnh có hoạt động xử lý dữ liệu cá nhân.

2. Hướng dẫn, hỗ trợ kỹ thuật cho các cơ quan, đơn vị trong việc:

- a) Quản lý tài khoản, phân quyền và kiểm soát truy cập;
- b) Bảo đảm an toàn trong lưu trữ, truyền đưa và trao đổi dữ liệu cá nhân;
- c) Ghi nhận, quản lý và bảo vệ nhật ký hệ thống;
- d) Sao lưu, khôi phục dữ liệu và bảo đảm tính sẵn sàng của hệ thống;

đ) Phát hiện, cảnh báo và xử lý các nguy cơ mất an toàn thông tin liên quan đến dữ liệu cá nhân.

3. Phối hợp với Công an tỉnh và các cơ quan, đơn vị trong việc ứng phó, khắc phục sự cố an toàn thông tin mạng có liên quan đến dữ liệu cá nhân theo chức năng, nhiệm vụ và thẩm quyền được giao.

4. Phối hợp rà soát, đánh giá mức độ an toàn của các hệ thống thông tin thuộc phạm vi quản lý của tỉnh có xử lý dữ liệu cá nhân; đề xuất nâng cấp, bổ sung biện pháp kỹ thuật phù hợp với mức độ rủi ro và yêu cầu bảo đảm an toàn hệ thống thông tin.

5. Hướng dẫn các cơ quan, đơn vị thực hiện các yêu cầu về bảo đảm an toàn hệ thống thông tin theo cấp độ và các quy định kỹ thuật có liên quan đến hoạt động xử lý, lưu trữ và truyền đưa dữ liệu cá nhân.

6. Phối hợp với Công an tỉnh và các cơ quan, đơn vị có liên quan trong việc rà soát, đánh giá và bảo đảm an toàn đối với các nền tảng, hệ thống dùng chung, cơ sở dữ liệu dùng chung và hạ tầng số của tỉnh có hoạt động xử lý dữ liệu cá nhân.

Điều 29. Trách nhiệm của Sở Nội vụ

1. Phối hợp với Công an tỉnh và các cơ quan, đơn vị có liên quan tham mưu Ủy ban nhân dân tỉnh về bố trí nhân sự, bộ phận bảo vệ dữ liệu cá nhân tại các cơ quan, đơn vị thuộc phạm vi quản lý theo quy định của pháp luật.

2. Phối hợp tổ chức hoặc tham mưu tổ chức đào tạo, bồi dưỡng, cập nhật kiến thức và nâng cao năng lực cho đội ngũ thực hiện nhiệm vụ bảo vệ dữ liệu cá nhân theo chức năng, nhiệm vụ được giao.

3. Phối hợp lồng ghép nội dung bảo vệ dữ liệu cá nhân trong các chương trình cải cách hành chính, chuyển đổi số và các chương trình, kế hoạch có liên quan theo quy định.

4. Phối hợp với Công an tỉnh và các cơ quan, đơn vị có liên quan trong việc theo dõi, đánh giá việc bố trí và thực hiện nhiệm vụ của nhân sự, bộ phận bảo vệ dữ liệu cá nhân theo quy định.

5. Phối hợp tham mưu việc biểu dương, khen thưởng tập thể, cá nhân có thành tích trong công tác bảo vệ dữ liệu cá nhân theo quy định của pháp luật về thi đua, khen thưởng.

Điều 30. Trách nhiệm của Sở Tài chính

1. Chủ trì, phối hợp với Công an tỉnh và các cơ quan, đơn vị có liên quan tham mưu Ủy ban nhân dân tỉnh bố trí kinh phí thực hiện công tác bảo vệ dữ liệu cá nhân theo phân cấp quản lý ngân sách nhà nước và quy định của pháp luật.

2. Hướng dẫn các cơ quan, đơn vị lập, tổng hợp, quản lý và sử dụng kinh phí thực hiện công tác bảo vệ dữ liệu cá nhân trong phạm vi dự toán ngân sách nhà nước được cấp có thẩm quyền giao.

3. Phối hợp tham mưu Ủy ban nhân dân tỉnh xem xét, bố trí nguồn lực thực hiện các nhiệm vụ bảo vệ dữ liệu cá nhân theo yêu cầu, nhiệm vụ và khả năng cân đối ngân sách địa phương.

4. Phối hợp kiểm tra việc quản lý, sử dụng kinh phí thực hiện nhiệm vụ bảo vệ dữ liệu cá nhân theo quy định của pháp luật về ngân sách nhà nước.

Điều 31. Trách nhiệm của các sở, ban, ngành, đơn vị thuộc phạm vi quản lý của Ủy ban nhân dân tỉnh

1. Người đứng đầu cơ quan, đơn vị chịu trách nhiệm tổ chức thực hiện công tác bảo vệ dữ liệu cá nhân trong phạm vi chức năng, nhiệm vụ và hoạt động xử lý dữ liệu cá nhân thuộc trách nhiệm quản lý.

2. Chỉ định nhân sự hoặc bộ phận bảo vệ dữ liệu cá nhân theo quy định; ban hành văn bản phân công nhiệm vụ, xác định rõ trách nhiệm của các bộ phận và cá nhân có liên quan.

3. Rà soát, xác định và quản lý danh mục dữ liệu cá nhân được thu thập, lưu trữ, xử lý; xác định mục đích, phạm vi, vai trò và biện pháp bảo vệ phù hợp đối với từng hoạt động xử lý.

4. Xây dựng, ban hành hoặc tổ chức thực hiện quy trình nội bộ về:

- a) Thu thập, xử lý và sử dụng dữ liệu cá nhân;
- b) Cung cấp, chia sẻ và chuyển giao dữ liệu cá nhân;
- c) Thực hiện quyền của chủ thể dữ liệu cá nhân;
- d) Quản lý quyền truy cập, khai thác và sử dụng dữ liệu cá nhân;
- đ) Lưu trữ, xóa, hủy dữ liệu cá nhân;
- e) Ứng phó và xử lý sự cố vi phạm quy định về bảo vệ dữ liệu cá nhân.

5. Bảo đảm các hệ thống thông tin, cơ sở dữ liệu và thiết bị có hoạt động xử lý dữ liệu cá nhân được áp dụng biện pháp bảo vệ phù hợp theo quy định của pháp luật về bảo vệ dữ liệu cá nhân, an toàn thông tin mạng và an ninh mạng.

6. Kiểm soát việc xử lý dữ liệu cá nhân của tổ chức, doanh nghiệp, nhà thầu, đơn vị cung cấp dịch vụ và các bên khác có liên quan; xác định rõ trách nhiệm bảo vệ dữ liệu cá nhân trong hợp đồng, thỏa thuận hoặc văn bản có liên quan.

7. Tổ chức tuyên truyền, phổ biến, đào tạo, bồi dưỡng và nâng cao nhận thức về bảo vệ dữ liệu cá nhân cho cán bộ, công chức, viên chức, người lao động thuộc phạm vi quản lý.

8. Kịp thời phát hiện, báo cáo, ứng phó và khắc phục sự cố; thực hiện nghĩa vụ thông báo vi phạm theo quy định của Luật Bảo vệ dữ liệu cá nhân, Nghị định số 356/2025/NĐ-CP và Chương IV của Quy chế này.

9. Chịu trách nhiệm trước pháp luật về hoạt động xử lý dữ liệu cá nhân thuộc phạm vi quản lý và việc thực hiện các trách nhiệm được giao theo Quy chế này.

10. Thực hiện chế độ báo cáo, cung cấp thông tin và phối hợp với Công an tỉnh, Sở Khoa học và Công nghệ và các cơ quan có liên quan trong công tác bảo vệ dữ liệu cá nhân theo quy định.

Điều 32. Trách nhiệm của Ủy ban nhân dân cấp xã

1. Tổ chức thực hiện Quy chế này và các quy định của pháp luật về bảo vệ dữ liệu cá nhân trong phạm vi quản lý.

2. Người đứng đầu Ủy ban nhân dân cấp xã chịu trách nhiệm tổ chức thực hiện công tác bảo vệ dữ liệu cá nhân đối với các hoạt động xử lý dữ liệu thuộc phạm vi quản lý của Ủy ban nhân dân cấp xã.

3. Chỉ định nhân sự hoặc bộ phận bảo vệ dữ liệu cá nhân phù hợp với quy mô, tính chất hoạt động xử lý dữ liệu, vị trí việc làm và điều kiện thực tế của địa phương.

4. Rà soát, xác định và quản lý dữ liệu cá nhân phát sinh trong quá trình giải quyết thủ tục hành chính, cung cấp dịch vụ công và thực hiện các nhiệm vụ quản lý nhà nước tại địa phương.

5. Thực hiện các biện pháp bảo vệ dữ liệu cá nhân trong hồ sơ giấy, hồ sơ điện tử, hệ thống thông tin, cơ sở dữ liệu và các phương tiện khác thuộc phạm vi quản lý.

6. Kiểm soát việc cung cấp, chia sẻ dữ liệu cá nhân giữa Ủy ban nhân dân cấp xã với các cơ quan, đơn vị khác; chỉ thực hiện khi có căn cứ pháp lý và đúng phạm vi, mục đích theo quy định.

7. Khi phát hiện sự cố hoặc vi phạm quy định về bảo vệ dữ liệu cá nhân, thực hiện ngay các biện pháp xử lý ban đầu, báo cáo theo quy định tại Chương IV của Quy chế và phối hợp với cơ quan có thẩm quyền để xử lý.

8. Thực hiện tuyên truyền, phổ biến và nâng cao nhận thức về bảo vệ dữ liệu cá nhân cho cán bộ, công chức, người lao động thuộc phạm vi quản lý.

9. Thực hiện chế độ báo cáo, cung cấp thông tin và phối hợp với Công an tỉnh và các cơ quan có liên quan trong công tác bảo vệ dữ liệu cá nhân theo quy định.

Điều 33. Trách nhiệm của cán bộ, công chức, viên chức và người lao động

1. Tuân thủ Luật Bảo vệ dữ liệu cá nhân, Nghị định số 356/2025/NĐ-CP, Quy chế này và các quy định nội bộ của cơ quan, đơn vị trong quá trình xử lý dữ liệu cá nhân.
2. Chỉ truy cập, khai thác, sử dụng dữ liệu cá nhân trong phạm vi nhiệm vụ, quyền hạn và quyền truy cập được cấp.
3. Không tự ý sao chép, sửa đổi, cung cấp, chia sẻ, chuyển giao, tiết lộ hoặc sử dụng dữ liệu cá nhân cho mục đích cá nhân hoặc mục đích khác không được phép.
4. Bảo vệ tài khoản, thông tin xác thực, thiết bị và phương tiện được giao; không cung cấp thông tin xác thực cho người khác sử dụng.
5. Kịp thời báo cáo người có thẩm quyền và bộ phận, nhân sự bảo vệ dữ liệu cá nhân khi phát hiện nguy cơ hoặc sự cố liên quan đến dữ liệu cá nhân.
6. Tham gia đầy đủ các chương trình đào tạo, tập huấn, phổ biến kiến thức và quy định về bảo vệ dữ liệu cá nhân do cơ quan, đơn vị tổ chức.
7. Chịu trách nhiệm theo quy định của pháp luật và quy định nội bộ của cơ quan, đơn vị đối với hành vi vi phạm trong quá trình xử lý dữ liệu cá nhân.

Điều 34. Trách nhiệm phối hợp giữa các cơ quan, đơn vị

1. Các cơ quan, đơn vị có trách nhiệm phối hợp trong việc thực hiện Quy chế này trên cơ sở chức năng, nhiệm vụ, quyền hạn được giao và bảo đảm nguyên tắc không chồng chéo, không làm thay chức năng của cơ quan, đơn vị khác.
2. Khi giải quyết vụ việc liên ngành hoặc vụ việc có liên quan đến nhiều cơ quan, đơn vị, cơ quan chủ trì có trách nhiệm xác định rõ nội dung, phạm vi, trách nhiệm của từng cơ quan, đơn vị tham gia phối hợp.
3. Cơ quan, đơn vị được đề nghị phối hợp có trách nhiệm cung cấp thông tin, tài liệu và thực hiện các nội dung thuộc chức năng, nhiệm vụ, quyền hạn của mình theo quy định của pháp luật.
4. Việc trao đổi, cung cấp thông tin giữa các cơ quan, đơn vị trong quá trình phối hợp phải bảo đảm đúng mục đích, phạm vi, thẩm quyền và các yêu cầu về bảo vệ dữ liệu cá nhân, bí mật nhà nước, an ninh mạng, an toàn thông tin và các quy định pháp luật có liên quan.
5. Công an tỉnh là đầu mối tổng hợp, tham mưu Ủy ban nhân dân tỉnh trong việc điều phối, hướng dẫn và theo dõi công tác phối hợp về bảo vệ dữ liệu cá nhân trên địa bàn tỉnh theo chức năng, nhiệm vụ và thẩm quyền được giao. Trong quá trình thực hiện, nếu có khó khăn, vướng mắc, các cơ quan, đơn vị phản ánh về Công an tỉnh để tổng hợp, báo cáo Ủy ban nhân dân tỉnh xem xét, sửa đổi, bổ sung cho phù hợp.