



Ký bởi TRUNG TÂM THÔNG TIN - CÔNG BÁO
VĂN PHÒNG ỦY BAN NHÂN DÂN, ỦY BAN NHÂN DÂN TỈNH
PHÚ THỌ

**ỦY BAN NHÂN DÂN
TỈNH PHÚ THỌ**

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

Số: 48/2026/QĐ-UBND

Phú Thọ, ngày 12 tháng 8 năm 2026

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 Phú Thọ**

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

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

Căn cứ Nghị định số 78/2025/NĐ-CP ngày 01 tháng 4 năm 2025 của Chính phủ quy định chi tiết một số điều và biện pháp để tổ chức, hướng dẫn thi hành Luật Ban hành văn bản quy phạm pháp luật năm 2025 được sửa đổi, bổ sung bởi Nghị định số 187/2025/NĐ-CP ngày 01 tháng 7 năm 2025 của Chính phủ;

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

Theo đề nghị của Giám đốc Công an tỉnh tại Tờ trình số 6854/TTr-CAT-ANM ngày 04 tháng 8 năm 2026;

Ủy ban nhân dân ban hành 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 Phú Thọ.

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 Phú Thọ.

Điều 2. Quyết định này có hiệu lực thi hành kể từ ngày 25 tháng 8 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 các xã, phường; các cơ quan và tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này./.

**TM. ỦY BAN NHÂN DÂN
CHỦ TỊCH**

Trần Duy Đông

QUY CHẾ

**Bảo vệ dữ liệu cá nhân trong hoạt động của
các cơ quan nhà nước trên địa bàn tỉnh Phú Thọ**
(Ban hành kèm theo Quyết định số 48/2026/QĐ-UBND)

Chương I QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh

- Quy chế này quy định về bảo vệ dữ liệu cá nhân trong hoạt động của các cơ quan nhà nước trên địa bàn tỉnh Phú Thọ.
- Các quy định về bảo vệ dữ liệu cá nhân không nêu trong Quy chế này thực hiện theo quy định của pháp luật hiện hành.
- Trong Quy chế này, các dẫn chiếu, tham chiếu đến các quy định hoặc văn bản quy phạm pháp luật khác được hiểu là bao gồm cả các văn bản hướng dẫn, sửa đổi, bổ sung hoặc điều chỉnh, thay thế liên quan đến quy định, văn bản được dẫn chiếu.

Điều 2. Đối tượng áp dụng

- Các cơ quan quản lý hành chính nhà nước và các đơn vị sự nghiệp công lập thuộc phạm vi quản lý của Ủy ban nhân dân tỉnh Phú Thọ có tham gia thu thập, xử lý, lưu trữ dữ liệu cá nhân (sau đây gọi tắt là cơ quan, đơn vị, địa phương).
- Cán bộ, công chức, viên chức, người lao động đang công tác trong các cơ quan, đơn vị, địa phương quy định tại khoản 1 Điều này; cơ quan, tổ chức, cá nhân được cơ quan, đơn vị, địa phương giao, thuê hoặc phối hợp thực hiện hoạt động thu thập, lưu trữ, xử lý dữ liệu cá nhân trong phạm vi Quy chế này.

Điều 3. Nguyên tắc bảo vệ dữ liệu cá nhân

- Bảo vệ dữ liệu cá nhân là yêu cầu bắt buộc, thường xuyên, liên tục, có tính xuyên suốt trong quá trình thu thập, xử lý, lưu trữ dữ liệu cá nhân. Bảo vệ dữ liệu cá nhân cần tuân thủ các nguyên tắc chung quy định tại Điều 3 Luật Bảo vệ dữ liệu cá nhân năm 2025.
- Cơ quan, tổ chức, cá nhân quy định tại Điều 2 Quy chế này có trách nhiệm chủ động, tự giác thực hiện công tác bảo vệ dữ liệu cá nhân; chấp hành nghiêm các quy định của pháp luật liên quan và các quy định tại Quy chế này.

Chương II QUY ĐỊNH CỤ THỂ

Điều 4. Xác định và phân loại dữ liệu cá nhân được xử lý

Căn cứ Điều 3 và Điều 4 Nghị định số 356/2025/NĐ-CP quy định chi tiết một số điều và biện pháp thi hành Luật Bảo vệ dữ liệu cá nhân, các cơ quan, đơn

vị, địa phương có trách nhiệm rà soát, phân loại đối với dữ liệu cá nhân do đơn vị mình thu thập, xử lý, lưu trữ (bao gồm dữ liệu cá nhân cơ bản và dữ liệu cá nhân nhạy cảm). Việc xử lý dữ liệu cá nhân nhạy cảm phải được thiết lập quy trình bảo vệ độc lập, phân quyền truy cập, khai thác nghiêm ngặt và tuân thủ các điều kiện chặt chẽ theo quy định trong Luật Bảo vệ dữ liệu cá nhân và các quy định pháp luật có liên quan.

1. Dữ liệu cá nhân được thu thập, lưu trữ, xử lý trong hoạt động của các cơ quan nhà nước trên địa bàn tỉnh bao gồm:

a) Dữ liệu cá nhân được tạo lập trong quá trình thực hiện chức năng, nhiệm vụ quản lý nhà nước của các cơ quan, đơn vị, địa phương thuộc tỉnh và theo các quy định của pháp luật khác có quy định cụ thể về chức năng, nhiệm vụ của các cơ quan, đơn vị, địa phương;

b) Dữ liệu cá nhân của cán bộ, công chức, viên chức, người lao động làm việc tại các cơ quan, đơn vị, địa phương trên địa bàn tỉnh theo quy định của pháp luật về công chức, viên chức và các quy định pháp luật khác có liên quan;

c) Thông tin về tài khoản số, tài khoản giao dịch điện tử của cá nhân và dữ liệu cá nhân phản ánh hoạt động, lịch sử hoạt động trên các hệ thống thông tin do các cơ quan, đơn vị, địa phương làm chủ quản theo quy định của pháp luật;

d) Các dữ liệu cá nhân khác phát sinh trong quá trình các cơ quan, đơn vị, địa phương thực hiện chức năng, nhiệm vụ, quyền hạn được giao mà không thuộc các quy định nêu tại điểm a, điểm b và điểm c khoản này.

2. Những trường hợp xử lý các dữ liệu cá nhân mà không cần sự đồng ý của chủ thể dữ liệu thực hiện theo quy định tại Điều 19 Luật Bảo vệ dữ liệu cá nhân năm 2025.

3. Việc xử lý dữ liệu cá nhân cần được sự đồng ý của chủ thể dữ liệu cá nhân thực hiện theo các trường hợp quy định tại Điều 9 và Điều 11 Luật Bảo vệ dữ liệu cá nhân năm 2025, trừ trường hợp pháp luật có quy định khác.

Điều 5. Xác định vai trò về bảo vệ dữ liệu cá nhân

1. Ủy ban nhân dân tỉnh Phú Thọ thực hiện vai trò là bên kiểm soát và xử lý dữ liệu cá nhân đối với:

a) Dữ liệu cá nhân được quy định tại điểm a và điểm b khoản 1 Điều 4 của Quy chế này, trừ các dữ liệu cá nhân thuộc các lĩnh vực được phân cấp quản lý cho các cơ quan, đơn vị, địa phương;

b) Thông tin về tài khoản số và dữ liệu cá nhân phản ánh lịch sử hoạt động của cá nhân trên các hệ thống thông tin do Ủy ban nhân dân tỉnh làm chủ quản (không bao gồm các hệ thống thông tin Ủy ban nhân dân tỉnh đã ủy quyền cho cơ quan, đơn vị khác quản lý, vận hành để thực hiện trách nhiệm chủ quản hệ thống thông tin).

2. Các cơ quan, đơn vị, địa phương thực hiện vai trò là bên kiểm soát và xử lý dữ liệu cá nhân đối với:

a) Dữ liệu cá nhân thuộc phạm vi chức năng, nhiệm vụ, lĩnh vực quản lý

nhà nước được phân cấp quản lý cho cơ quan, đơn vị, địa phương mình; dữ liệu cá nhân được tạo lập trong quá trình thực hiện chức năng, nhiệm vụ đã được Ủy ban nhân dân tỉnh phân cấp, ủy quyền cho cơ quan, đơn vị, địa phương thực hiện theo quy định pháp luật;

b) Thông tin về tài khoản số và dữ liệu cá nhân phản ánh lịch sử hoạt động của cá nhân trên các hệ thống thông tin do cơ quan, đơn vị, địa phương làm chủ quản hoặc được Ủy ban nhân dân tỉnh ủy quyền thực hiện trách nhiệm của chủ quản hệ thống thông tin.

3. Cơ quan, đơn vị, địa phương nào có hoạt động xử lý dữ liệu cá nhân mà chưa được xác định tại khoản 1 và khoản 2 Điều này thì Thủ trưởng đơn vị đó có trách nhiệm căn cứ tính chất, mục đích, phạm vi hoạt động xử lý dữ liệu cá nhân của đơn vị mình để xác định vai trò là “bên kiểm soát dữ liệu cá nhân”, “bên kiểm soát và xử lý dữ liệu cá nhân” hoặc “bên xử lý dữ liệu cá nhân” theo quy định của Luật Bảo vệ dữ liệu cá nhân; pháp luật có liên quan và thông báo cho Công an tỉnh để theo dõi, tổng hợp chung.

Điều 6. Bảo vệ dữ liệu cá nhân trong quá trình xử lý dữ liệu cá nhân trên hệ thống thông tin lưu trữ, xử lý dữ liệu cá nhân

1. Cơ quan, đơn vị, địa phương sử dụng hệ thống thông tin có chức năng lưu trữ, xử lý dữ liệu cá nhân có trách nhiệm xác định chính xác các cá nhân được cấp quyền truy cập hệ thống để thực hiện nhiệm vụ xử lý dữ liệu cá nhân; phải thực hiện ngay việc gửi đề nghị thay đổi, thu hồi tài khoản truy cập hệ thống thông tin đến đơn vị vận hành hệ thống thông tin ngay sau khi có sự thay đổi về nhân sự hoặc phân công công tác, nhiệm vụ liên quan đến xử lý dữ liệu cá nhân tại cơ quan, đơn vị, địa phương.

2. Cá nhân được cấp tài khoản truy cập hệ thống thông tin để xử lý dữ liệu cá nhân có trách nhiệm:

a) Bảo mật thông tin xác thực (mật khẩu, thiết bị mã hóa hoặc phương tiện xác thực khác) của tài khoản được cấp; không cung cấp thông tin xác thực cho người không có thẩm quyền hoặc không được giao nhiệm vụ đối với hệ thống thông tin;

b) Chỉ thực hiện các hoạt động xử lý dữ liệu cá nhân trong phạm vi nhiệm vụ được giao; không tự ý khai thác, sử dụng dữ liệu cá nhân trên hệ thống ngoài phạm vi trách nhiệm, nhiệm vụ được phân công;

c) Khi không còn được phân công thực hiện nhiệm vụ xử lý dữ liệu cá nhân trên hệ thống thông tin, phải đề nghị cơ quan, đơn vị thu hồi tài khoản hoặc thay đổi quyền truy cập để cấp mới hoặc phân quyền lại tài khoản cho người tiếp nhận nhiệm vụ theo phân công.

Điều 7. Bảo vệ dữ liệu cá nhân trong quá trình xử lý dữ liệu cá nhân ngoài hệ thống thông tin lưu trữ, xử lý dữ liệu cá nhân

1. Việc xử lý dữ liệu cá nhân ngoài các hệ thống thông tin điện tử bao gồm dữ liệu dạng bản giấy, thư điện tử, dữ liệu lưu trữ trong thiết bị lưu trữ ngoại vi và các trường hợp khác theo quy định của pháp luật phải tuân thủ các yêu cầu sau:

a) Xác định căn cứ pháp luật cho việc xử lý dữ liệu cá nhân: trước khi xử lý, phải xác định rõ cơ sở pháp lý cho mục đích và phạm vi dữ liệu cá nhân được phép xử lý bằng cách dẫn chiếu cụ thể điều, khoản của văn bản quy phạm pháp luật cho phép việc thu thập, xử lý dữ liệu đó;

b) Trường hợp nhận được yêu cầu thu thập, xử lý dữ liệu cá nhân nằm ngoài phạm vi được pháp luật quy định, đơn vị thực hiện phải làm rõ cơ sở thực hiện với bên yêu cầu xử lý; đồng thời phải có sự đồng ý của chủ thể dữ liệu trước khi tiến hành xử lý dữ liệu ngoài phạm vi nói trên.

2. Công chức, viên chức được phân công xử lý dữ liệu cá nhân có trách nhiệm thực hiện đầy đủ các biện pháp bảo đảm an toàn, bảo mật trong quá trình xử lý, cụ thể như sau:

a) Không cung cấp hoặc chia sẻ dữ liệu cá nhân đã thu thập cho bất kỳ tổ chức, cá nhân nào không thuộc phạm vi được phép cung cấp theo quy định của pháp luật;

b) Sử dụng trang thiết bị, máy tính đảm bảo an toàn, an ninh thông tin khi xử lý dữ liệu cá nhân: máy tính phải được dán tem an ninh an toàn và cài đặt phần mềm phòng chống mã độc; thường xuyên cập nhật các bản vá lỗ hổng bảo mật (nếu có); phải được kiểm tra, đánh giá an ninh mạng định kỳ theo quy định;

c) Trường hợp được phép thực hiện trao đổi dữ liệu cá nhân trên môi trường mạng hoặc mang dữ liệu cá nhân ra khỏi cơ quan, đơn vị, địa phương bằng thiết bị, phương tiện điện tử (trừ dữ liệu thuộc danh mục bí mật nhà nước thực hiện theo quy định của pháp luật về bảo vệ bí mật nhà nước), cần phải áp dụng biện pháp mã hóa tệp dữ liệu và các biện pháp an toàn khác theo quy định pháp luật. Không sử dụng mạng xã hội để trao đổi dữ liệu cá nhân, trừ trường hợp được sự đồng ý của chủ thể dữ liệu;

d) Kiểm soát chặt chẽ các loại hình dữ liệu cá nhân ở dạng điện tử và dạng phi điện tử; chủ động thiết lập, giới hạn quyền tiếp cận dữ liệu cá nhân trong phạm vi những người được phân công xử lý; thực hiện các biện pháp xóa an toàn dữ liệu hoặc hủy vật lý thiết bị lưu trữ, xử lý dữ liệu cá nhân sau khi hoàn thành mục đích sử dụng, hết hạn lưu trữ theo quy định hoặc không còn nhu cầu sử dụng thiết bị.

3. Thủ trưởng các cơ quan, đơn vị, địa phương có trách nhiệm ban hành hoặc tổ chức triển khai thực hiện quy trình nội bộ trong quá trình xử lý dữ liệu cá nhân ngoài hệ thống thông tin lưu trữ, xử lý dữ liệu cá nhân đảm bảo theo đúng quy định tại khoản 1 và khoản 2 Điều 7 trong Quy chế này và quy định của pháp luật có liên quan.

Điều 8. Bảo đảm an toàn hệ thống thông tin xử lý dữ liệu cá nhân

1. Thực hiện bảo đảm an toàn, an ninh mạng đối với hệ thống thông tin theo cấp độ và bảo vệ an ninh mạng đối với các hệ thống thông tin xử lý dữ liệu cá nhân theo đúng quy định của pháp luật về an ninh mạng, trong đó hệ thống thông tin phải đáp ứng các yêu cầu bảo vệ ở cấp độ tương ứng theo quy định hiện hành; tuân thủ các tiêu chuẩn, quy chuẩn kỹ thuật về an ninh mạng. Đối với các dự án đầu tư, nâng cấp hệ thống thông tin xử lý dữ liệu cá nhân sau khi Quy chế này có hiệu lực, cơ quan chủ trì dự án phải đánh giá và nêu rõ căn cứ pháp luật cho việc

xử lý dữ liệu cá nhân ngay trong giai đoạn đề xuất chủ trương đầu tư, lập dự án hoặc kế hoạch thuê dịch vụ công nghệ thông tin;

2. Trang bị và duy trì các hệ thống giám sát an ninh mạng, hệ thống ngăn chặn thoát dữ liệu đối với hệ thống thông tin có xử lý dữ liệu cá nhân từ cấp độ 3 trở lên để theo dõi liên tục hoạt động của hệ thống mạng, máy chủ; các hệ thống này phải được cấu hình để phát hiện các hành vi bất thường hoặc truy cập trái phép vào dữ liệu và đưa ra cảnh báo sớm để có biện pháp xử lý kịp thời;

3. Hệ thống thông tin xử lý dữ liệu cá nhân phải có tính năng ghi và lưu trữ nhật ký hệ thống trong quá trình xử lý dữ liệu cá nhân; khuyến khích thiết kế hiển thị trên giao diện người dùng thông tin về căn cứ pháp lý của việc xử lý dữ liệu cá nhân để người dùng biết và tuân thủ mục đích, phạm vi cho phép;

4. Áp dụng các biện pháp xác thực và mã hóa đối với kênh kết nối truyền đưa dữ liệu cá nhân giữa các hệ thống thông tin với nhau, cũng như giữa người dùng với hệ thống thông tin;

5. Áp dụng các giải pháp, phần mềm phòng chống mã độc trên máy chủ và máy trạm của hệ thống thông tin xử lý dữ liệu cá nhân. Không sử dụng dữ liệu cá nhân thật trên môi trường thử nghiệm; không được phép xử lý dữ liệu cá nhân trên hệ thống thông tin thử nghiệm; trường hợp cần thử nghiệm, phải sử dụng dữ liệu giả định hoặc đã ẩn danh, để tránh rủi ro lộ lọt dữ liệu cá nhân;

6. Tổ chức đánh giá an ninh, an toàn đối với hệ thống thông tin định kỳ nhằm nhận diện các lỗ hổng bảo mật, điểm yếu trong hệ thống, từ đó áp dụng các biện pháp khắc phục, phòng ngừa rủi ro tương ứng. Việc kiểm tra, đánh giá an ninh mạng định kỳ đối với hệ thống thông tin xử lý dữ liệu cá nhân phải đồng thời bao gồm kiểm tra việc tuân thủ quy định pháp luật về bảo vệ dữ liệu cá nhân, bên cạnh việc kiểm tra về an toàn, an ninh mạng theo quy định chung;

7. Định kỳ bảo trì, bảo dưỡng, nâng cấp phần cứng, phần mềm của hệ thống thông tin; kịp thời cập nhật các bản vá bảo mật cho hệ điều hành, cơ sở dữ liệu và ứng dụng nhằm duy trì, cải thiện hiệu suất và tính bảo mật của hệ thống. Các trang thiết bị thuộc hệ thống thông tin có chức năng thu thập, lưu trữ, xử lý dữ liệu cá nhân phải được kiểm tra an ninh thông tin trước khi đưa vào sử dụng và sau khi tiến hành bảo dưỡng, sửa chữa, nâng cấp;

8. Thực hiện xóa an toàn toàn bộ dữ liệu cá nhân trên hệ thống thông tin khi hệ thống kết thúc vận hành, chấm dứt sử dụng hoặc cần thay thế bằng hệ thống khác, trừ trường hợp pháp luật cho phép hoặc yêu cầu lưu trữ để chuyển sang hệ thống mới.

Điều 9. Bảo vệ dữ liệu cá nhân trong hoạt động biên tập, công khai thông tin trên trang/cổng thông tin điện tử, dịch vụ công trực tuyến

Cơ quan, đơn vị, địa phương vận hành trang/cổng thông tin điện tử, dịch vụ công trực tuyến có trách nhiệm triển khai các biện pháp kiểm soát, ngăn ngừa việc hiển thị hoặc công khai trái phép dữ liệu cá nhân trên các cổng thông tin này. Tuyệt đối không để lộ lọt, công khai dữ liệu cá nhân trái quy định từ hoạt động cung cấp thông tin trên trang/cổng thông tin điện tử, dịch vụ công trực tuyến và trong quá

trình biên tập nội dung đăng tải. Cụ thể, cần thực hiện các biện pháp sau:

1. Bổ sung vào quy trình biên tập tin, bài, phóng sự việc rà soát dữ liệu cá nhân trong nội dung và thực hiện “kiểm duyệt 02 bước” qua bộ phận chuyên trách về công nghệ thông tin và công tác bảo vệ dữ liệu cá nhân trước khi đăng trên trang/cổng thông tin điện tử, dịch vụ công trực tuyến. Tuyệt đối không đăng công khai các thông tin chứa dữ liệu cá nhân nhạy cảm nếu không thực sự cần thiết;

2. Rà soát, bảo đảm các trường thông tin được hiển thị công khai trên trang/cổng thông tin điện tử, dịch vụ công trực tuyến không vi phạm quy định về bảo vệ dữ liệu cá nhân; kịp thời gỡ bỏ thông tin không cần thiết hoặc có nguy cơ gây lộ, lọt dữ liệu cá nhân;

3. Khuyến khích tích hợp, hiển thị chức năng cảnh báo rủi ro lộ lọt dữ liệu cá nhân đối với các chuyên mục có khả năng công khai thông tin do chủ thể dữ liệu cá nhân tự nhập liệu trên trang/cổng thông tin điện tử, dịch vụ công trực tuyến; áp dụng các công cụ kỹ thuật bao gồm AI, bộ lọc từ khóa hoặc công cụ khác để kiểm soát việc hiển thị nội dung có chứa dữ liệu cá nhân trên trang/cổng thông tin điện tử, dịch vụ công trực tuyến;

4. Khi phát hiện nội dung đã công khai có chứa dữ liệu cá nhân không đúng quy định, cơ quan, đơn vị, địa phương thực hiện đăng tải phải ngay lập tức gỡ bỏ, vô hiệu hóa nội dung đăng tải. Đồng thời xác định trách nhiệm của tổ chức, cá nhân có liên quan, đánh giá mức độ vi phạm và xem xét xử lý theo quy định tại Quy chế này.

Điều 10. Xử lý và thông báo vi phạm pháp luật về bảo vệ dữ liệu cá nhân

1. Khi phát hiện cá nhân thuộc cơ quan, đơn vị mình quản lý có hành vi vi phạm quy định về bảo vệ dữ liệu cá nhân, Thủ trưởng cơ quan, đơn vị trực tiếp quản lý cá nhân vi phạm có trách nhiệm xem xét, xử lý như sau:

a) Nếu cá nhân vi phạm thuộc thẩm quyền quản lý của Ủy ban nhân dân tỉnh, cơ quan, đơn vị trực tiếp quản lý cá nhân đó phối hợp Văn phòng Ủy ban nhân dân tỉnh, Công an tỉnh đánh giá, xác định mức độ vi phạm; phối hợp Sở Nội vụ báo cáo Ủy ban nhân dân tỉnh xem xét, quyết định hình thức xử lý phù hợp;

b) Nếu cá nhân vi phạm thuộc thẩm quyền quản lý của cơ quan, đơn vị, địa phương thì Thủ trưởng cơ quan, đơn vị trực tiếp quản lý cá nhân vi phạm tiến hành đánh giá mức độ vi phạm và quyết định biện pháp xử lý kỷ luật phù hợp theo quy định pháp luật hiện hành;

c) Đối với các trường hợp vi phạm không thuộc phạm vi quy định tại điểm a và điểm b khoản này, Thủ trưởng cơ quan, đơn vị trực tiếp quản lý cá nhân vi phạm có trách nhiệm xác định mức độ vi phạm và quyết định biện pháp xử lý phù hợp theo quy định của pháp luật hiện hành;

d) Trường hợp phát hiện hành vi vi phạm có dấu hiệu cấu thành vi phạm quy định pháp luật về bảo vệ dữ liệu cá nhân, cơ quan/người có thẩm quyền xử lý kỷ luật đối với cá nhân vi phạm (theo phân cấp quản lý cán bộ, công chức, viên chức) phải thông báo ngay cho Bộ Công an (qua Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao) và Công an tỉnh (qua Phòng An ninh

mạng và phòng, chống tội phạm sử dụng công nghệ cao) để phối hợp xử lý.

2. Trường hợp phát hiện hành vi vi phạm quy định bảo vệ dữ liệu cá nhân trên địa bàn tỉnh do các đối tượng không thuộc quyền quản lý của tỉnh thực hiện:

a) Nếu hành vi vi phạm thuộc phạm vi quản lý của Ủy ban nhân dân tỉnh và không được phân cấp cho cơ quan, đơn vị, địa phương thì sở, ban, ngành có liên quan phối hợp với Công an tỉnh (qua Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao) đánh giá, xác định mức độ vi phạm và báo cáo, tham mưu Ủy ban nhân dân tỉnh có biện pháp xử lý theo quy định của pháp luật;

b) Nếu hành vi vi phạm thuộc phạm vi quản lý của các cơ quan, đơn vị, địa phương thì giao các cơ quan, đơn vị, địa phương đánh giá, xác định mức độ vi phạm để báo cáo Ủy ban nhân dân tỉnh chỉ đạo đồng thời trao đổi, phối hợp Công an tỉnh (qua Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao) để có phương án xử lý theo quy định pháp luật.

3. Trong vòng 72 giờ kể từ khi phát hiện vi phạm đối với trường hợp thuộc diện phải thông báo, cơ quan có thẩm quyền phải gửi Thông báo vi phạm đến Cơ quan chuyên trách bảo vệ dữ liệu cá nhân của Bộ Công an; đồng thời báo cáo Ủy ban nhân dân tỉnh và áp dụng ngay các biện pháp ngăn chặn, khắc phục hậu quả kịp thời theo quy định. Quy trình, cách thức, biểu mẫu, nơi nhận thông báo thực hiện theo Điều 23 Luật Bảo vệ dữ liệu cá nhân và theo Điều 28, Điều 29 Nghị định số 356/2025/NĐ-CP. Công an tỉnh tham mưu, giúp Ủy ban nhân dân tỉnh theo dõi, đôn đốc việc thông báo này khi có vụ việc vi phạm xảy ra trên địa bàn tỉnh.

CHƯƠNG III

TRÁCH NHIỆM TRONG CÔNG TÁC BẢO VỆ DỮ LIỆU CÁ NHÂN

Điều 11. Trách nhiệm của Công an tỉnh

1. Tham mưu Ủy ban nhân dân tỉnh về công tác bảo vệ dữ liệu cá nhân trên địa bàn tỉnh và chịu trách nhiệm tham mưu, giúp Ủy ban nhân dân tỉnh trong công tác quản lý nhà nước về bảo vệ dữ liệu cá nhân trên địa bàn tỉnh.

2. Tham mưu giúp Ủy ban nhân dân tỉnh tổ chức triển khai công tác bảo vệ dữ liệu cá nhân trong phạm vi toàn tỉnh; hướng dẫn, đôn đốc, kiểm tra, đánh giá các cơ quan, đơn vị trong việc thực hiện Quy chế này và tuân thủ các quy định pháp luật, hướng dẫn của Bộ Công an về bảo vệ dữ liệu cá nhân. Kịp thời báo cáo, đề xuất Chủ tịch Ủy ban nhân dân tỉnh sửa đổi, bổ sung Quy chế này khi cần thiết, nhằm bảo đảm phù hợp với các quy định, tiêu chuẩn, quy chuẩn kỹ thuật liên quan và với tình hình thực tế triển khai tại địa phương.

3. Phối hợp với các cơ quan, đơn vị tổ chức tuyên truyền, phổ biến và nâng cao nhận thức của cán bộ, công chức, viên chức, các tổ chức, cá nhân khác trong phạm vi quản lý của tỉnh về các quy định pháp luật về bảo vệ dữ liệu cá nhân trên địa bàn tỉnh.

4. Tham mưu Ủy ban nhân dân tỉnh hướng dẫn, kiểm tra, đôn đốc các cơ quan, đơn vị, địa phương đảm bảo việc đáp ứng các quy định về bảo vệ dữ liệu cá nhân đối với các hệ thống thông tin do Ủy ban nhân dân tỉnh làm chủ quản (ngoại trừ các hệ thống thông tin Ủy ban nhân dân tỉnh đã ủy quyền cho đơn vị khác quản

lý theo quy định riêng).

5. Tham mưu Ủy ban nhân dân tỉnh thực hiện chế độ thông tin, báo cáo, tổng hợp về công tác bảo vệ dữ liệu cá nhân trên địa bàn tỉnh định kỳ và khi có yêu cầu của các cơ quan cấp trên có thẩm quyền theo quy định.

6. Chỉ định đơn vị, bộ phận chuyên trách và nhân sự chuyên trách công tác bảo vệ dữ liệu cá nhân tại Công an tỉnh để thực hiện nhiệm vụ đầu mối tham mưu, phối hợp triển khai công tác bảo vệ dữ liệu cá nhân trên địa bàn tỉnh.

7. Phối hợp kiểm tra an ninh thông tin theo thẩm quyền đối với các trang thiết bị thuộc hệ thống thông tin có chức năng thu thập, xử lý, lưu trữ dữ liệu cá nhân trước khi đưa vào sử dụng và sau khi tiến hành bảo dưỡng, sửa chữa, nâng cấp.

8. Kịp thời thông báo các lỗ hổng bảo mật có nguy cơ gây lộ, lọt dữ liệu cá nhân được phát hiện và các phương thức, thủ đoạn đánh cắp, chiếm đoạt, thu thập, sử dụng, mua bán, công khai hóa trái phép dữ liệu cá nhân; chủ động trong công tác phát hiện, phòng ngừa, đấu tranh, ngăn chặn các loại tội phạm và các hành vi vi phạm pháp luật xâm phạm an ninh dữ liệu và thông tin cá nhân trên địa bàn tỉnh.

9. Tham mưu Ủy ban nhân dân tỉnh tổ chức tập huấn, hướng dẫn áp dụng, tuân thủ và thi hành các quy định của pháp luật về bảo vệ dữ liệu cá nhân; hỗ trợ các cơ quan, đơn vị, địa phương giải quyết, khắc phục sự cố liên quan công tác bảo vệ dữ liệu cá nhân khi có yêu cầu.

10. Phối hợp các cơ quan, đơn vị, địa phương và các lực lượng chức năng trong công tác xác minh, điều tra, xử lý các trường hợp vi phạm về công tác bảo vệ dữ liệu cá nhân theo thẩm quyền và theo quy định của pháp luật.

Điều 12. Trách nhiệm của các cơ quan, đơn vị, địa phương

1. Tổ chức triển khai, giám sát và kiểm tra việc thực hiện Quy chế này và các quy định pháp luật về bảo vệ dữ liệu cá nhân tại cơ quan, đơn vị mình và các đơn vị trực thuộc (nếu có). Thường xuyên phổ biến, quán triệt tới toàn thể cán bộ, công chức, viên chức thuộc phạm vi quản lý về quyền và nghĩa vụ trong bảo vệ dữ liệu cá nhân, xác định rõ trách nhiệm phải thực hiện và tiến độ thời gian theo quy định của pháp luật.

2. Rà soát, đánh giá các quy trình thu thập, xử lý dữ liệu cá nhân trong phạm vi quản lý; kịp thời đề xuất ban hành các biện pháp quản lý phù hợp với quy mô, mức độ xử lý dữ liệu cá nhân của cơ quan, đơn vị mình. Kiên quyết xử lý nghiêm các hành vi chuyển giao, mua bán dữ liệu cá nhân trái phép nếu phát hiện trong lĩnh vực, địa bàn mình quản lý.

3. Báo cáo tình hình bảo vệ dữ liệu cá nhân theo yêu cầu của cơ quan nhà nước có thẩm quyền; đồng thời gửi báo cáo cho Công an tỉnh để tổng hợp, báo cáo theo quy định.

4. Chỉ định bằng văn bản bộ phận hoặc cá nhân phụ trách công tác bảo vệ dữ liệu cá nhân của cơ quan, đơn vị có trách nhiệm chính trong bảo đảm các hệ thống thông tin do đơn vị làm chủ quản (hoặc được Ủy ban nhân dân tỉnh ủy quyền quản lý) đáp ứng yêu cầu về bảo vệ dữ liệu cá nhân theo quy định, đồng

thời là đầu mỗi thực hiện chế độ báo cáo khi có yêu cầu.

5. Trường hợp đơn vị thực hiện vai trò bên kiểm soát dữ liệu, bên kiểm soát và xử lý dữ liệu hoặc bên xử lý dữ liệu cá nhân, đơn vị phải thực hiện các trách nhiệm tương ứng được quy định tại Luật Bảo vệ dữ liệu cá nhân và Nghị định số 356/2025/NĐ-CP và tại Quy chế này.

6. Thủ trưởng các cơ quan, đơn vị chịu trách nhiệm trước Chủ tịch Ủy ban nhân dân tỉnh về việc ban hành hoặc tổ chức triển khai thực hiện quy trình nội bộ, quản trị hệ thống thông tin, kiểm tra đánh giá và xử lý vi phạm về bảo vệ dữ liệu cá nhân tại cơ quan, đơn vị mình quản lý, bảo đảm tuân thủ đúng quy định của pháp luật và Quy chế này.

Điều 13. Trách nhiệm của cán bộ, công chức, viên chức và người lao động trong các cơ quan, đơn vị

1. Tuân thủ nghiêm các quy định của pháp luật về bảo vệ dữ liệu cá nhân và các quy định tại Quy chế này trong quá trình thực thi nhiệm vụ.

2. Thực hiện đúng quyền và nghĩa vụ của chủ thể dữ liệu đối với dữ liệu cá nhân của bản thân theo quy định pháp luật.

3. Chủ động áp dụng các biện pháp bảo vệ dữ liệu cá nhân trong phạm vi công việc của mình; khi phát hiện dữ liệu cá nhân có nguy cơ bị lộ, lọt hoặc không được bảo vệ đúng quy định, phải báo cáo ngay với bộ phận phụ trách và yêu cầu đơn vị quản lý dữ liệu có biện pháp khắc phục kịp thời, đúng quy định.

4. Thông báo kịp thời cho thủ trưởng cơ quan, đơn vị về các trường hợp vi phạm quy định bảo vệ dữ liệu cá nhân xảy ra tại đơn vị. Chịu trách nhiệm trước pháp luật và trước cơ quan quản lý về những vi phạm hoặc tổn thất, mất mát dữ liệu cá nhân do mình gây ra do không tuân thủ các quy định của Quy chế này và của pháp luật liên quan.

Điều 14. Trách nhiệm của các tổ chức, cá nhân liên quan

1. Các tổ chức, cá nhân liên quan trong quá trình thu thập, lưu trữ, xử lý dữ liệu cá nhân trong hoạt động của các cơ quan, đơn vị, địa phương phải tuân thủ Quy chế này và các quy định hiện hành của pháp luật về bảo vệ dữ liệu cá nhân.

2. Cơ quan, tổ chức, cá nhân vi phạm quy định về bảo vệ dữ liệu cá nhân sẽ bị xem xét xử lý kỷ luật và bị xử phạt vi phạm hành chính hoặc truy cứu trách nhiệm hình sự theo quy định của pháp luật, tùy theo tính chất, mức độ vi phạm. Trường hợp gây thiệt hại cho người có dữ liệu cá nhân bị xâm phạm thì phải bồi thường theo quy định của Bộ luật Dân sự và các quy định pháp luật có liên quan.

CHƯƠNG IV TỔ CHỨC THỰC HIỆN

Điều 15. Trách nhiệm thi hành

1. Căn cứ Quy chế này, Thủ trưởng, người đứng đầu các cơ quan, đơn vị, địa phương quy định tại khoản 1 Điều 2 Quy chế này có trách nhiệm tổ chức triển khai

thực hiện trong phạm vi quản lý. Định kỳ 6 tháng (trước ngày 15 tháng 6), hằng năm (trước ngày 15 tháng 12) hoặc khi có yêu cầu đột xuất, các đơn vị báo cáo Ủy ban nhân dân tỉnh kết quả triển khai, thực hiện Quy chế (qua Công an tỉnh).

2. Công an tỉnh có trách nhiệm theo dõi, đôn đốc, kiểm tra, đánh giá việc thực hiện Quy chế, báo cáo Ủy ban nhân dân tỉnh theo định kỳ hoặc đột xuất theo yêu cầu của cơ quan có thẩm quyền.

3. Các nội dung liên quan tới bảo vệ dữ liệu cá nhân chưa được quy định tại Quy chế này hoặc chưa có sự thống nhất với Quy chế này và quy định pháp luật hiện hành thì thực hiện theo quy định của pháp luật.

4. Các cơ quan, đơn vị, địa phương chủ động rà soát các hệ thống thông tin xử lý dữ liệu cá nhân được giao quản lý và tổ chức triển khai thực hiện các phương án bảo đảm các hệ thống thông tin trên đáp ứng các yêu cầu về công tác bảo vệ dữ liệu cá nhân quy định tại Quy chế này.

5. Trong quá trình thực hiện Quy chế này, nếu phát sinh khó khăn, vướng mắc, không phù hợp, các cơ quan, đơn vị, địa phương và tổ chức, cá nhân có liên quan phản ánh kịp thời về Công an tỉnh để tổng hợp báo cáo Ủy ban nhân dân tỉnh xem xét điều chỉnh, bổ sung.

Điều 16. Kinh phí thực hiện

1. Kinh phí công tác bảo vệ dữ liệu cá nhân được bố trí từ nguồn ngân sách nhà nước và các nguồn kinh phí hợp pháp khác.

2. Kinh phí thực hiện bảo đảm theo phân cấp ngân sách hiện hành, được bố trí trong dự toán ngân sách hàng năm của cơ quan, đơn vị, địa phương theo quy định./.