

QUY CHẾ

**Bảo vệ dữ liệu cá nhân trong hoạt động của cơ quan nhà nước
trên địa bàn thành phố Đồng Nai**
(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 về bảo vệ dữ liệu cá nhân và trách nhiệm của cơ quan, đơn vị, địa phương, tổ chức, cá nhân có liên quan đến bảo vệ dữ liệu cá nhân trong hoạt động của cơ quan nhà nước, đơn vị sự nghiệp thuộc thành phố Đồng Nai.

2. Các quy định về bảo vệ dữ liệu cá nhân không quy định trong Quy chế này thực hiện theo quy định của pháp luật hiện hành.

Điều 2. Đối tượng áp dụng

1. Các Sở, ban, ngành và các đơn vị sự nghiệp thuộc phạm vi quản lý của thành phố, Ủy ban nhân dân các xã, phường (sau đây gọi tắt là cơ quan, đơn vị, địa phương).

2. Cán bộ, công chức, viên chức và người lao động đang công tác trong các cơ quan, đơn vị, địa phương nêu tại khoản 1 Điều này và các tổ chức, cá nhân có liên quan áp dụng Quy chế này trong quá trình thu thập, lưu trữ, xử lý dữ liệu cá nhân trong hoạt động của các cơ quan, đơn vị, địa phương.

Chương II QUY ĐỊNH CỤ THỂ

Điều 3. Xác định và phân loại dữ liệu cá nhân được xử lý trong các cơ quan nhà nước của thành phố

1. Các cơ quan, đơn vị, địa phương có hoạt động lưu trữ, xử lý dữ liệu cá nhân có trách nhiệm rà soát, phân loại, lập danh mục dữ liệu cá nhân đang xử lý (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 của Luật Bảo vệ dữ liệu cá nhân số 91/2025/QH15 và các quy định pháp luật có liên quan.

2. Dữ liệu cá nhân được thu thập, lưu trữ, xử lý trong hoạt động của các cơ

quan nhà nước trên địa bàn thành phố bao gồm:

a) Dữ liệu cá nhân được thu thập, tiếp nhận, tạo lập, lưu trữ, quản lý, khai thác trong quá trình thực hiện chức năng, nhiệm vụ, quyền hạn được giao theo quy định pháp luật.

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 thành phố theo quy định của pháp luật về cán bộ, 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) 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 trường hợp quy định tại điểm a, b và c khoản này.

3. Các trường hợp xử lý dữ liệu cá nhân mà không cần sự đồng ý của chủ thể dữ liệu:

a) Xử lý dữ liệu cá nhân thuộc điểm a, b và c khoản 2 Điều này.

b) Xử lý dữ liệu cá nhân thu được từ việc ghi âm, ghi hình công cộng theo quy định tại Điều 32, Luật số 91/2025/QH15.

c) Trường hợp xử lý dữ liệu cá nhân khác không cần sự đồng ý của chủ thể dữ liệu theo quy định tại Điều 19 Luật số 91/2025/QH15.

Điều 4. Xác định vai trò về bảo vệ dữ liệu cá nhân trong cơ quan nhà nước trên địa bàn thành phố

Cơ quan, đơn vị, địa phương có hoạt động xử lý dữ liệu cá nhân căn cứ quy định pháp luật có trách nhiệm chủ động xác định vai trò là “Bên kiểm soát dữ liệu cá nhân”, “Bên xử lý dữ liệu cá nhân” và “Bên kiểm soát và xử lý dữ liệu cá nhân”, đồng thời phải được thể hiện bằng hồ sơ, văn bản phân công, thỏa thuận chia sẻ dữ liệu hoặc hợp đồng xử lý dữ liệu đối với: dữ liệu cá nhân được thu thập, lưu trữ, xử lý thuộc phạm vi chức năng, nhiệm vụ được giao theo quy định; dữ liệu cá nhân được thu thập, lưu trữ, xử lý trong quá trình thực hiện chức năng, nhiệm vụ được quy định tại khoản 2 Điều 5 của Quy chế này.

Điều 5. 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 xử lý dữ liệu cá nhân có trách nhiệm xác định cá nhân được cấp quyền truy cập

hệ thống để thực hiện nhiệm vụ xử lý dữ liệu cá nhân truy cập theo hướng đúng người, đúng nhiệm vụ, đúng phạm vi, đúng thời hạn và bảo đảm nguyên tắc phân quyền tối thiểu. Khi có thay đổi về nhân sự được phân công công việc liên quan đến xử lý dữ liệu cá nhân, phải điều chỉnh hoặc thu hồi ngay quyền truy cập của người dùng đó.

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 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) Chỉ xử lý dữ liệu cá nhân trên các trang thiết bị, máy tính trong hệ thống thông tin xử lý dữ liệu cá nhân được bảo đảm an toàn, an ninh mạng theo quy định pháp luật.

d) Khi không còn nhiệm vụ xử lý dữ liệu cá nhân trên hệ thống, phải yêu cầu đơn vị quản lý hệ thống thu hồi hoặc thay đổi quyền truy cập kịp thời.

Điều 6. 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 bên ngoài các hệ thống thông tin phải tuân thủ các yêu cầu sau:

a) Trước khi thu thập, lưu trữ, xử lý dữ liệu cá nhân, phải xác định rõ cơ sở pháp lý cho mục đích và phạm vi dữ liệu cá nhân được phép xử lý.

b) Trường hợp nhận được yêu cầu thu thập, xử lý dữ liệu cá nhân 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.

c) Không được sử dụng tài khoản cá nhân, mạng xã hội, ứng dụng nhắn tin công cộng hoặc phương tiện không được cơ quan có thẩm quyền cho phép để trao đổi, truyền đưa dữ liệu cá nhân trong hoạt động công vụ.

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 ngoài phạm vi được phép cung cấp theo quy định của pháp luật.

b) 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.

c) Kiểm soát chặt chẽ các phiên bản 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 việc lập biên bản ghi nhận việc áp dụng 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.

Điều 7. Bảo đảm an toàn hệ thống thông tin thu thập, lưu trữ, xử lý dữ liệu cá nhân

Các hệ thống thông tin của cơ quan, đơn vị, địa phương có thu thập, lưu trữ, xử lý dữ liệu cá nhân phải thực hiện yêu cầu bảo đảm an toàn hệ thống thông tin như sau:

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 thu thập, lưu trữ, xử lý dữ liệu cá nhân theo đúng quy định của pháp luật về an ninh mạng. 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 hệ thống thông tin do Ủy ban nhân dân thành phố làm chủ quản, thực hiện theo các quy định tại Quy chế bảo đảm an ninh mạng của Ủy ban nhân dân thành phố (nếu có); đối với hệ thống thông tin do cơ quan, đơn vị cấp dưới làm chủ quản hoặc được phân cấp, ủy quyền quản lý theo quy định pháp luật thì thực hiện theo quy chế bảo đảm an ninh mạng của đơn vị chủ quản đó.

2. Áp dụng các biện pháp xác thực, mã hóa để bảo vệ dữ liệu cá nhân trong quá trình truyền đưa qua các kênh kết nối giữa các hệ thống thông tin với nhau và giữa người dùng với hệ thống thông tin.

3. Hệ thống thông tin thu thập, lưu trữ, 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 để hiển thị trên giao diện người dùng thông tin về căn cứ pháp lý của việc xử lý dữ liệu cá nhân.

4. Các thành phần, thiết bị, phần mềm, ứng dụng thuộc hệ thống thông tin có chức năng thu thập, lưu trữ, xử lý dữ liệu cá nhân phải được kiểm tra, đánh giá an ninh mạng trước khi đưa vào vận hành và được kiểm tra, đánh giá định kỳ hoặc đột xuất khi có thay đổi cấu hình, phát sinh sự cố, sửa chữa, bảo dưỡng theo yêu cầu của cơ quan có thẩm quyền và phải bao gồm kiểm tra việc tuân thủ quy định pháp luật về bảo vệ dữ liệu cá nhân; kịp thời phát hiện các lỗ hổng bảo mật, điểm yếu trong hệ thống thông tin, triển khai, áp dụng các biện pháp tương ứng để khắc phục, phòng ngừa rủi ro, nguy cơ lộ, mất dữ liệu cá nhân.

5. Không được xử lý dữ liệu cá nhân trên hệ thống thông tin thử nghiệm hoặc trong quá trình thử nghiệm giải pháp phần mềm, trừ trường hợp được cho phép theo quy định. Trường hợp cần thử nghiệm, chỉ được phép sử dụng dữ liệu không phải dữ liệu cá nhân, dữ liệu cá nhân đã được khử nhận dạng hoặc áp dụng kỹ thuật ẩn danh dữ liệu cá nhân tuân theo quy chuẩn và quy định của pháp luật.

6. Triển khai các giải pháp, phần mềm phòng chống mã độc trên máy chủ và máy trạm của hệ thống thông tin thu thập, lưu trữ, xử lý dữ liệu cá nhân tuân thủ quy định pháp luật về an ninh mạng. 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, duy trì, cải thiện hiệu suất và tính bảo mật của hệ thống.

7. Cơ quan, đơn vị quản lý hệ thống thông tin thu thập, lưu trữ, xử lý dữ liệu cá nhân có trách nhiệm trang bị và duy trì các hệ thống giám sát an ninh mạng, hệ thống ngăn chặn thất thoát dữ liệu đối với hệ thống thông tin 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.

8. Thực hiện xóa an toàn toàn bộ dữ liệu cá nhân trên hệ thống thông tin thu thập, lưu trữ, xử lý dữ liệu cá nhân khi hệ thống kết thúc vận hành, trừ trường hợp được phép lưu trữ theo quy định pháp luật.

Điều 8. Bảo vệ dữ liệu cá nhân đối với cổng, trang thông tin điện tử, dịch vụ công trực tuyến

Các cơ quan, đơn vị quản lý, vận hành cổng, trang thông tin điện tử, cổng dịch vụ công trực tuyến của thành phố có trách nhiệm triển khai các biện pháp kiểm soát, ngăn ngừa việc hiển thị hoặc công khai dữ liệu cá nhân không đúng quy định trên các cổng, trang thông tin điện tử này; rà soát dữ liệu cá nhân trong nội dung, biểu mẫu, hồ sơ, tài khoản, chức năng tra cứu thông tin trước khi đăng tải hoặc cung cấp cho người sử dụng. Cụ thể, cần thực hiện các biện pháp sau:

1. Bổ sung vào quy trình biên tập tin, bài viết yêu cầu phải rà soát dữ liệu cá nhân trong nội dung bài viết trước khi đăng trên cổng, trang thông tin điện tử. Không đăng công khai dữ liệu cá nhân nhạy cảm trên cổng, trang thông tin điện tử, dịch vụ công trực tuyến, trừ trường hợp pháp luật quy định.

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

3. Khuyến khích tích hợp chức năng hiển thị cảnh báo rủi ro lộ lọt dữ liệu cá nhân đối với các chuyên mục có khả năng công khai thông tin do người dùng nhập. Trường hợp người dùng có xu hướng nhập thông tin chứa dữ liệu cá nhân, hệ thống nên cảnh báo về nguy cơ lộ lọt. Đồng thời, áp dụng các công cụ kỹ thuật để kiểm soát việc hiển thị nội dung có chứa dữ liệu cá nhân trên cổng, trang thông tin điện tử, dịch vụ công trực tuyến của thành phố.

Điều 9. Phân loại và quy trình ứng phó sự cố

1. Phân loại mức độ sự cố

a) Mức độ 1 (Bình thường): lỗi kỹ thuật nhỏ, chưa gây rò rỉ dữ liệu.

b) Mức độ 2 (Nghiêm trọng): rò rỉ dữ liệu cá nhân cơ bản hoặc thông tin quan trọng nội bộ của 01 đơn vị.

c) Mức độ 3 (Đặc biệt nghiêm trọng): rò rỉ dữ liệu nhạy cảm quy mô lớn, thông tin quan trọng ảnh hưởng ở phạm vi toàn thành phố hoặc bị tấn công mã hóa tống tiền (Ransomware).

2. Quy trình ứng phó sự cố

a) Ngay khi phát hiện dấu hiệu bị tấn công hoặc lộ lọt dữ liệu, đơn vị phải báo cáo ngay cho Công an thành phố qua đường dây nóng trong vòng 30 phút, đồng thời gửi thông báo/báo cáo ban đầu qua thư điện tử hoặc liên hệ trực tiếp với Bộ phận thường trực của Đội ứng cứu sự cố (Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao, Công an thành phố) và cơ quan chủ quản hệ thống thông tin để được hỗ trợ, xử lý (tối đa trong 06 giờ).

Đối với các trường hợp hệ thống thông tin của chính quyền địa phương (do các Sở, ngành, Ủy ban nhân dân các cấp quản lý) có lưu trữ, xử lý dữ liệu phối hợp liên quan đến công tác tổ chức, xây dựng Đảng hoặc thông tin của cán bộ, công chức, đảng viên thuộc diện cấp ủy quản lý; khi xảy ra sự cố mất an toàn thông tin hoặc lộ lọt dữ liệu. Yêu cầu đơn vị chủ quản hệ thống ngoài việc báo cáo Công an thành phố theo quy định cần nhanh chóng thông tin cho Thường trực cấp ủy cùng cấp (thông qua Văn phòng cấp ủy) để kịp thời phối hợp xử lý, ổn

định tình hình và đánh giá các rủi ro về mặt chính trị.

b) Công an thành phố chủ trì phối hợp đơn vị vận hành phong tỏa hệ thống, thu thập chứng cứ và thực hiện các biện pháp “ngắt kết nối khẩn cấp” để bảo vệ dữ liệu cốt lõi.

Chương III **TRÁCH NHIỆM CỦA CÁC CƠ QUAN, ĐƠN VỊ** **CÓ LIÊN QUAN TRONG BẢO VỆ DỮ LIỆU CÁ NHÂN**

Điều 10. Trách nhiệm chung

1. Mỗi cơ quan, đơn vị phải phân công Lãnh đạo phụ trách và bố trí nhân sự hoặc đầu mối thực hiện công tác bảo vệ dữ liệu cá nhân phù hợp với quy mô, tính chất, mức độ xử lý dữ liệu của cơ quan, đơn vị, danh sách phải gửi về Công an thành phố để theo dõi.

2. Cán bộ, công chức, viên chức được cấp tài khoản có quyền quản trị hệ thống hoặc có quyền truy cập vào danh mục dữ liệu nhạy cảm hoặc tham gia xử lý dữ liệu tại bộ phận Một cửa phải sử dụng định danh điện tử cấp độ 2 và thực hiện ký số cho mỗi giao dịch liên quan đến dữ liệu cá nhân, thông tin quan trọng.

Điều 11. Trách nhiệm của Công an thành phố

Công an thành phố là cơ quan tham mưu, giúp Ủy ban nhân dân thành phố quản lý nhà nước về bảo vệ dữ liệu cá nhân trên địa bàn thành phố, có trách nhiệm:

1. Tham mưu, giúp Ủy ban nhân dân thành phố tổ chức triển khai công tác bảo vệ dữ liệu cá nhân trong phạm vi toàn thành phố; 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.

2. Phối hợp Sở Khoa học và Công nghệ cùng tiến hành giám sát an ninh mạng: triển khai hệ thống giám sát 24/7 đối với toàn bộ các luồng truy cập ra/vào Trung tâm tích hợp dữ liệu thành phố. Phát hiện và ngăn chặn các dấu hiệu tấn công mạng, xâm nhập trái phép, mã độc và các nguy cơ mất an toàn thông tin.

3. Phối hợp Sở Khoa học và Công nghệ thực hiện kiểm tra, đánh giá an ninh mạng đối với các hệ thống thông tin, ứng dụng của thành phố trước khi cho phép kết nối vào Trung tâm tích hợp dữ liệu thành phố.

4. 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 thành phố về các quy định pháp luật về bảo vệ dữ liệu cá nhân trên địa bàn thành phố.

5. Hướng dẫn, đôn đốc các cơ quan, đơn vị được Ủy ban nhân dân thành phố giao trực tiếp quản lý, vận hành hệ thống thông tin do Ủy ban nhân dân thành

phổ làm chủ quản (ngoại trừ các hệ thống thông tin Ủy ban nhân dân thành phố đã phân cấp, ủy quyền cho đơn vị khác quản lý theo quy định) triển khai các biện pháp bảo vệ dữ liệu cá nhân, bảo đảm hệ thống thông tin đáp ứng quy định của pháp luật về bảo vệ dữ liệu cá nhân và Quy chế này.

6. Thực hiện chế độ thông tin, báo cáo, tổng hợp về công tác bảo vệ dữ liệu cá nhân trên địa bàn, trình Ủy ban nhân dân thành phố để gửi báo cáo cho các cơ quan cấp trên có thẩm quyền theo quy định.

7. Chỉ định đơn vị, bộ phận chuyên trách và nhân sự phụ trách công tác bảo vệ dữ liệu cá nhân tại Công an thành phố để thực hiện nhiệm vụ đầu mối triển khai, hướng dẫn, giám sát việc bảo vệ dữ liệu cá nhân trong phạm vi toàn thành phố. Thông tin về bộ phận và cán bộ phụ trách được thông báo tới Cơ quan chuyên trách bảo vệ dữ liệu cá nhân của Bộ Công an và Ủy ban nhân dân thành phố để tham mưu, phối hợp thực hiện về công tác bảo vệ dữ liệu cá nhân trên địa bàn thành phố.

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

9. Chủ trì, phối hợp các cơ quan, đơn vị, địa phương có liên quan tham mưu đề xuất cho Ủy ban nhân dân thành phố, Chủ tịch Ủy ban nhân dân thành phố xem xét biểu dương, khen thưởng thành tích trong công tác bảo vệ dữ liệu cá nhân (nếu có) theo quy định của pháp luật hiện hành.

Điều 12. Trách nhiệm của Sở Khoa học và Công nghệ

1. Bảo đảm hệ thống điện nguồn, điều hòa nhiệt độ, phòng cháy chữa cháy và hệ thống lưu trữ dữ liệu tại Trung tâm tích hợp dữ liệu thành phố vận hành liên tục.

2. Thực hiện cập nhật, vá lỗi phần mềm định kỳ hằng tháng cho các máy chủ và nền tảng ảo hóa.

3. Thường xuyên sao lưu dữ liệu của Trung tâm tích hợp dữ liệu thành phố. Bảo đảm có ít nhất 03 bản sao lưu dữ liệu, trong đó có 02 bản sử dụng 02 phương tiện lưu trữ khác nhau và 01 bản lưu tại vị trí vật lý khác ngoài trụ sở Trung tâm tích hợp dữ liệu thành phố (theo chiến lược 3-2-1).

4. Phối hợp bàn giao các luồng dữ liệu nhật ký hệ thống và nhật ký truy cập cho Công an thành phố qua cổng kết nối an toàn định kỳ hoặc theo thời gian thực.

Điều 13. Trách nhiệm của Sở Tài chính

Phối hợp với Công an thành phố và các cơ quan, đơn vị liên quan tham mưu cho Ủy ban nhân dân thành phố cân đối, bố trí kinh phí phục vụ hoạt động bảo vệ

dữ liệu cá nhân theo phân cấp quản lý ngân sách nhà nước và quy định của pháp luật về ngân sách nhà nước hiện hành.

Điều 14. Trách nhiệm của Sở Nội vụ

Phối hợp với Công an thành phố và các cơ quan có liên quan tham mưu, đề xuất Chủ tịch Ủy ban nhân dân thành phố khen thưởng thành tích trong công tác bảo vệ dữ liệu cá nhân (nếu có) theo quy định của pháp luật hiện hành về thi đua, khen thưởng trên địa bàn thành phố.

Điều 15. Trách nhiệm của các sở, ban, ngành, đơn vị thành phố và Ủy ban nhân dân các xã, phường

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).

2. Rà soát, đánh giá các quy trình thu thập, xử lý dữ liệu cá nhân trong phạm vi quản lý, thực hiện các biện pháp bảo vệ dữ liệu cá nhân phù hợp với quy mô, mức độ xử lý dữ liệu cá nhân của cơ quan, đơn vị mình. Kịp thời thông báo cho cơ quan có thẩm quyền khi phát hiện các hành vi chuyển giao, mua bán trái phép dữ liệu cá nhân thuộc phạm vi quản lý.

3. Định kỳ, đột xuất 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 thành phố thực hiện công tác tham mưu, giúp Ủy ban nhân dân thành phố thực hiện công tác quản lý nhà nước về bảo vệ dữ liệu cá nhân trên địa bàn thành phố.

4. Rà soát, bố trí nhân sự, giao đầu mối hoặc bộ phận thực hiện bảo vệ dữ liệu cá nhân của đơn vị, bảo đảm đáp ứng điều kiện năng lực và yêu cầu chuyên môn về bảo vệ dữ liệu cá nhân, được tham gia bồi dưỡng, tập huấn về bảo vệ dữ liệu cá nhân theo quy định của pháp luật.

5. Chủ động rà soát, đánh giá các hệ thống thông tin thu thập, lưu trữ, xử lý dữ liệu cá nhân thuộc phạm vi quản lý; phối hợp với Công an thành phố trong việc hướng dẫn, kiểm tra, đánh giá và triển khai các nội dung, phương án của đơn vị, địa phương trong bảo đảm hệ thống thông tin thu thập, lưu trữ, xử lý dữ liệu cá nhân đáp ứng quy định của pháp luật và Quy chế này; định kỳ thực hiện kiểm tra, đánh giá an ninh mạng đối với các thành phần phần cứng, phần mềm đối với hệ thống thông tin thu thập, lưu trữ, xử lý dữ liệu cá nhân thuộc đơn vị, địa phương quản lý.

6. 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 số 91/2025/QH15, 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 và Quy chế này.

7. Trường hợp cơ quan, đơn vị, địa phương trong thành phố ký kết thỏa thuận hoặc hợp đồng với tổ chức, cá nhân khác để thực hiện hoạt động xử lý dữ liệu cá nhân (thuộc trường hợp được cho phép theo quy định pháp luật), đơn vị đó có trách nhiệm yêu cầu bên xử lý dữ liệu cá nhân cung cấp thông tin, tài liệu liên quan đến Hồ sơ đánh giá tác động xử lý dữ liệu cá nhân do bên xử lý dữ liệu cá nhân thực hiện để phục vụ quản lý nhà nước (nếu hoạt động xử lý dữ liệu cá nhân thuộc trường hợp phải đánh giá tác động theo quy định). Trong hợp đồng hoặc thỏa thuận với bên xử lý dữ liệu cá nhân, gồm: mục đích xử lý, phạm vi dữ liệu, thời hạn xử lý, biện pháp bảo mật, trách nhiệm thông báo sự cố, trách nhiệm xóa/hủy hoặc hoàn trả dữ liệu sau khi kết thúc hợp đồng, trách nhiệm bồi thường và cơ chế kiểm tra, giám sát. Công an thành phố là đơn vị tham mưu, giúp Ủy ban nhân dân thành phố tổng hợp các hồ sơ này để phục vụ công tác giám sát chung và tham mưu thực hiện công tác bảo vệ dữ liệu cá nhân trên địa bàn thành phố.

Điều 16. Trách nhiệm của người đứng đầu, người được giao nhiệm vụ thu thập, lưu trữ, xử lý dữ liệu cá nhân trong hoạt động của các cơ quan, đơn vị, địa phương

1. Thủ trưởng các cơ quan, đơn vị; Giám đốc các Sở, ban, ngành; Chủ tịch Ủy ban nhân dân các xã, phường chịu trách nhiệm trước Ủy ban nhân dân thành phố, Chủ tịch Ủy ban nhân dân thành phố về việc đảm bảo công tác 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.

2. Cán bộ, công chức, viên chức, người lao động trong các cơ quan nhà nước trên địa bàn thành phố có trách nhiệm:

a) 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.

b) 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.

c) 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.

d) 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.

Chương IV

KIỂM TRA, KHEN THƯỞNG VÀ XỬ LÝ VI PHẠM

Điều 17. Kiểm tra định kỳ, kiểm tra đột xuất

1. Công an thành phố thực hiện kiểm tra an ninh dữ liệu định kỳ 06 tháng/lần và có quyền kiểm tra đột xuất không cần báo trước đối với các đơn vị đang quản lý dữ liệu cá nhân theo thẩm quyền, trình tự, thủ tục do pháp luật quy định hoặc theo chỉ đạo của Ủy ban nhân dân thành phố, Chủ tịch Ủy ban nhân dân thành phố.

2. Kết quả kiểm tra là một trong những căn cứ để xem xét, đánh giá xếp loại thi đua của đơn vị và cá nhân hàng năm.

Điều 18. Khen thưởng và xử lý vi phạm

1. Đơn vị, cá nhân có thành tích xuất sắc trong việc phát hiện và ngăn chặn sự cố rò rỉ dữ liệu hoặc có sáng kiến, giải pháp, mô hình hiệu quả trong bảo vệ dữ liệu cá nhân sẽ được khen thưởng theo quy định của thành phố.

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 (đối với cán bộ, công chức, viên chức) 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.

Điều 19. Thông báo vi phạm quy định về bảo vệ dữ liệu cá nhân

Khi phát hiện dấu hiệu hành vi vi phạm quy định về bảo vệ dữ liệu cá nhân hoặc dấu hiệu vi phạm trong hoạt động xử lý dữ liệu cá nhân, cơ quan, đơn vị, địa phương phối hợp xác định, thông báo, xử lý như sau:

1. Bên kiểm soát dữ liệu cá nhân hoặc bên kiểm soát và xử lý dữ liệu cá nhân thực hiện thông báo vi phạm về bảo vệ dữ liệu cá nhân theo khoản 2 Điều này. Trường hợp chưa xác định được trách nhiệm thông báo vi phạm quy định về bảo vệ dữ liệu cá nhân thì báo cáo Ủy ban nhân dân thành phố (qua Công an thành phố) để phối hợp đánh giá, xác định chủ thể thực hiện trách nhiệm thông báo vi phạm về bảo vệ dữ liệu cá nhân theo khoản 2 Điều này.

2. Thông báo vi phạm quy định về bảo vệ dữ liệu cá nhân cho Bộ Công an thực hiện theo Điều 23 Luật số 91/2025/QH15 và Điều 28 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 (trong vòng 72 giờ kể từ khi phát hiện vi phạm, cơ quan có thẩm quyền phải gửi Thông báo vi phạm theo Mẫu

08 tại phụ lục kèm theo Nghị định số 356/2025/NĐ-CP đến Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao). Công an thành phố tham mưu, giúp Ủy ban nhân dân thành phố thực hiện theo dõi, đôn đốc việc thông báo này khi có vụ việc vi phạm xảy ra trên địa bàn thành phố.

Chương V **TỔ CHỨC THỰC HIỆN**

Điều 20. Trách nhiệm thực hiện

1. Thủ trưởng, người đứng đầu các cơ quan, đơn vị, địa phương có trách nhiệm phổ biến, quán triệt đến cán bộ, công chức, viên chức, người lao động thuộc phạm vi quản lý các quy định của pháp luật về bảo vệ dữ liệu cá nhân và Quy chế này để thực hiện. Định kỳ trước ngày 15/12 hằng năm báo cáo Ủy ban nhân dân thành phố (qua Công an thành phố) kết quả thực hiện.

2. Trong quá trình thực hiện Quy chế này, nếu phát sinh khó khăn, vướng mắc, các cơ quan, đơn vị, địa phương và tổ chức, cá nhân có liên quan kịp thời báo cáo Ủy ban nhân dân thành phố (qua Công an thành phố) để xem xét, giải quyết hoặc sửa đổi, bổ sung, thay thế Quy chế này cho phù hợp với yêu cầu thực tiễn và quy định của pháp luật.