TCVN **TIÊU CHUẨN QUỐC GIA**

DỰ THẢO

TCVN XXXXX:2026
ISO/IEC 29100:2024

Xuất bản lần 1

CÔNG NGHỆ THÔNG TIN - KỸ THUẬT AN TOÀN - KHUNG QUYỀN RIÊNG TƯ

Information technology - Security techniques - Privacy framework

HÀ NỘI – 2026

MỤC LỤC

Lời nói đầu

TCVN XXXXX: 2026 hoàn toàn tương đương với ISO/IEC ISO/IEC 29100:2024.

TCVN XXXXX: 2026 do Ban Cơ yếu Chính phủ biên soạn, Bộ Quốc phòng đề nghị, Ủy ban Tiêu chuẩn Đo lường Chất lượng Quốc gia thẩm định, Bộ Khoa học và Công nghệ công bố.

Lời giới thiệu

Tiêu chuẩn này cung cấp một khung ở mức tổng thể nhằm bảo vệ thông tin nhận dạng cá nhân (PII) trong các hệ thống công nghệ thông tin và truyền thông (ICT). Khung này mang tính khái quát và đặt các khía cạnh về tổ chức, kỹ thuật và thủ tục vào trong một khung bảo vệ quyền riêng tư tổng thể.

Khung quyền riêng tư này hỗ trợ các tổ chức xác định các yêu cầu bảo vệ quyền riêng tư liên quan đến PII trong môi trường ICT bằng cách:

— Xác định hệ thuật ngữ chung về quyền riêng tư;

— Xác định các tác nhân và vai trò của họ trong quá trình xử lý PII;

— Mô tả các yêu cầu bảo vệ quyền riêng tư; và

— Viện dẫn các nguyên tắc quyền riêng tư đã được công nhận.

Do số lượng công nghệ thông tin và truyền thông xử lý thông tin nhận dạng cá nhân (PII) ngày càng tăng, việc có các tiêu chuẩn an ninh thông tin quốc tế cung cấp sự hiểu biết chung về bảo vệ PII là rất quan trọng. Tiêu chuẩn này nhằm mục đích nâng cao các tiêu chuẩn an ninh hiện có bằng cách bổ sung trọng tâm liên quan đến việc xử lý PII.

Việc sử dụng và giá trị thương mại ngày càng tăng của PII, việc chia sẻ PII giữa các khu vực pháp lý, và sự phức tạp ngày càng tăng của các hệ thống CNTT, có thể gây khó khăn cho một tổ chức trong việc đảm bảo quyền riêng tư và tuân thủ các luật có thể áp dụng được. Các bên liên quan đến quyền riêng tư có thể ngăn chặn sự không chắc chắn và mất lòng tin bằng cách xử lý các vấn đề về quyền riêng tư một cách đúng đắn và tránh các trường hợp lạm dụng PII.

Việc áp dụng tiêu chuẩn này sẽ:

— Hỗ trợ thiết kế, triển khai, vận hành và bảo trì các hệ thống công nghệ thông tin và truyền thông xử lý và bảo vệ PII;

— Khuyến khích các giải pháp sáng tạo nhằm bảo vệ PII trong các hệ thống ICT; và
— Cải thiện các chương trình bảo vệ quyền riêng tư của tổ chức thông qua việc áp dụng các thực hành tốt nhất.

Khung quyền riêng tư được trình bày trong tiêu chuẩn này có thể được sử dụng làm cơ sở cho các sáng kiến tiêu chuẩn hóa bổ sung về quyền riêng tư, chẳng hạn như:

— Xây dựng kiến trúc tham chiếu kỹ thuật;

— Triển khai và sử dụng các công nghệ quyền riêng tư cụ thể cũng như quản lý quyền riêng tư tổng thể;

— Các biện pháp kiểm soát quyền riêng tư đối với các quy trình xử lý dữ liệu được thuê ngoài;

— Đánh giá rủi ro về quyền riêng tư hoặc

— Các thông số kỹ thuật cụ thể.

TIÊU CHUẨN QUỐC GIA **TCVN XXXXX:YYYY**

Công nghệ thông tin - Kỹ thuật an toàn - Khung quyền riêng tư

Information technology - Security techniques - Privacy framework

1 Phạm vi áp dụng

Tiêu chuẩn này đưa ra một khung quyền riêng tư nhằm:

— Quy định hệ thuật ngữ chung về quyền riêng tư;

— Xác định các tác nhân và vai trò của chúng trong việc xử lý thông tin nhận dạng cá nhân (PII);

— Mô tả các nội dung cần xem xét để bảo vệ quyền riêng tư;

— Viện dẫn các nguyên tắc quyền riêng tư đã biết trong lĩnh vực công nghệ thông tin.

Tiêu chuẩn này áp dụng cho các thể nhân và tổ chức tham gia vào việc xác định, mua sắm, kiến trúc, thiết kế, phát triển, thử nghiệm, bảo trì, quản trị và vận hành các hệ thống hoặc dịch vụ công nghệ thông tin và truyền thông, trong đó cần áp dụng các biện pháp kiểm soát quyền riêng tư cho việc xử lý PII.

2 Tài liệu viện dẫn

Không có tài liệu viện bắt buộc dẫn trong tiêu chuẩn này.

3 Thuật ngữ và định nghĩa

Trong phạm vi áp dụng của tài liệu này, các thuật ngữ và định nghĩa sau đây được áp dụng.

3.1

Tính ẩn danh (anonymity)

Đặc tính của thông tin không cho phép xác định trực tiếp hoặc gián tiếp một chủ thể thông tin nhận dạng cá nhân (PII) (3.9).

3.2

Ẩn danh hóa (Anonymization)

Quá trình làm thay đổi thông tin nhận dạng cá nhân (PII) (3.7) theo cách không thể khôi phục lại, để từ đó không còn có thể xác định được chủ thể PII (3.9), dù xác định trực tiếp hay gián tiếp, kể cả khi bên kiểm soát PII tự thực hiện hoặc kết hợp với bất kỳ bên nào khác.

3.3

Dữ liệu ẩn danh (anonymized data)

Là dữ liệu được tạo ra từ quá trình ẩn danh hóa thông tin nhận dạng cá nhân (PII) (3.7), theo định nghĩa tại (3.2).

3.4

Sự chấp thuận (consent)

Sự đồng ý tự nguyện, cụ thể và có hiểu biết của chủ thể thông tin nhận dạng cá nhân (PII) (3.9) về việc xử lý PII của họ.

3.5

Khả năng xác định danh tính (identifiability)

Điều kiện dẫn đến việc một chủ thể thông tin nhận dạng cá nhân (PII) (3.9) được xác định, trực tiếp hoặc gián tiếp, dựa trên một tập hợp PII nhất định.

3.6

Đăng ký tham gia (opt-in)

Quy trình hoặc loại chính sách theo đó chủ thể thông tin nhận dạng cá nhân (PII) (3.9) được yêu cầu thực hiện hành động để bày tỏ sự chấp thuận (3.4) rõ ràng, trước đó (3.4) cho việc xử lý PII của họ cho một mục đích cụ thể.

Chú thích 1: Một thuật ngữ khác thường được sử dụng cùng với nguyên tắc quyền riêng tư "chấp thuận và lựa chọn" là **"opt-out"**. Thuật ngữ này mô tả một quy trình hoặc loại chính sách theo đó chủ thể PII phải thực hiện một hành động riêng để từ chối hoặc rút lại sự chấp thuận, hoặc phản đối một hình thức xử lý cụ thể. Việc áp dụng chính sách opt-out mặc nhiên giả định rằng bên kiểm soát PII có quyền xử lý PII theo cách dự kiến. Quyền này có thể được suy ra từ một hành động nào đó của chủ thể PII khác với sự chấp thuận (ví dụ như việc đặt hàng trên một cửa hàng trực tuyến).

3.7

Thông tin nhận dạng cá nhân PII (personally identifiable information PII)

Thông tin (a) có thể được sử dụng để thiết lập mối liên hệ giữa thông tin đó và thể nhân mà thông tin đó liên quan đến, hoặc (b) có hoặc có thể có mối liên hệ trực tiếp hoặc gián tiếp với thể nhân đó.

Chú thích 1: "Thể nhân" trong định nghĩa này chính là **chủ thể thông tin nhận dạng cá nhân (PII)** (3.9). Khi xem xét liệu một chủ thể PII **có thể được xác định hay không**, cần tính đến tất cả các cách thức mà bên đang nắm giữ dữ liệu, hoặc bất kỳ bên nào khác, **có thể sử dụng một cách hợp lý** để liên kết tập hợp PII với thể nhân đó.

3.8

Bên kiểm soát PII (PII controller)

Là bên liên quan đến quyền riêng tư (hoặc các bên liên quan đến quyền riêng tư) quyết định mục đích và cách thức xử lý thông tin nhận dạng cá nhân (PII) (3.7), không bao gồm các thể nhân sử dụng dữ liệu cho mục đích cá nhân.

Chú thích 1:

Trong một số trường hợp, bên kiểm soát PII có thể chỉ định các bên khác (ví dụ như bên xử lý PII (3.10)) thay mặt mình thực hiện việc xử lý PII; tuy nhiên, trách nhiệm đối với việc xử lý vẫn thuộc về bên kiểm soát PII.

3.9

Chủ thể thông tin nhận dạng cá nhân (PII principal)

(chủ thể dữ liệu – data subject)

Là thể nhân mà thông tin nhận dạng cá nhân (PII) (3.7) liên quan tới.

3.10

Bên xử lý PII (PII processor)

Là bên liên quan đến quyền riêng tư, có trách nhiệm thực hiện việc xử lý thông tin nhận dạng cá nhân (PII) (3.7) thay mặt cho bên kiểm soát PII (3.8) và theo đúng chỉ đạo của bên kiểm soát PII.

3.11

Vi phạm quyền riêng tư (Privacy breach)

Là tình huống trong đó việc xử lý thông tin nhận dạng cá nhân (PII) (3.7) vi phạm một hoặc nhiều yêu cầu về bảo vệ quyền riêng tư.

3.12

Kiểm soát quyền riêng tư (Privacy control)

Là biện pháp được áp dụng để hạn chế rủi ro về quyền riêng tư, bằng cách làm giảm khả năng xảy ra hoặc giảm mức độ ảnh hưởng của rủi ro đó.

Chú thích 1:

Biện pháp kiểm soát quyền riêng tư có thể là biện pháp về tổ chức, vật lý hoặc kỹ thuật, chẳng hạn như chính sách, quy trình, hướng dẫn, hợp đồng pháp lý, cách thức quản lý hoặc cơ cấu tổ chức.

Chú thích 2:

Thuật ngữ kiểm soát cũng có thể được hiểu là biện pháp bảo vệ hoặc biện pháp phòng ngừa.

3.13

Công nghệ tăng cường quyền riêng tư PET (Privacy enhancing technology PET)

Kiểm soát quyền riêng tư (3.12), bao gồm các biện pháp, sản phẩm hoặc dịch vụ công nghệ thông tin và truyền thông (ICT), được sử dụng để bảo vệ quyền riêng tư bằng cách loại bỏ hoặc giảm bớt thông tin nhận dạng cá nhân (PII) (3.7), hoặc ngăn chặn việc xử lý PII không cần thiết và/hoặc không mong muốn, đồng thời vẫn bảo đảm không làm mất các chức năng của hệ thống ICT.

Chú thích 1:

Các công nghệ tăng cường quyền riêng tư có thể là, nhưng không chỉ giới hạn ở các công cụ ẩn danh hóa (3.2) và giả danh hóa (3.22), giúp loại bỏ, làm giảm, che giấu hoặc làm cho PII không còn khả năng nhận dạng, hoặc ngăn chặn việc xử lý PII không cần thiết, không được phép và/hoặc không mong muốn.

Chú thích 2:

Che giấu (masking) là quá trình che khuất các thành phần của PII.

3.14

Chính sách quyền riêng tư (Privacy Policy)

Ý định và định hướng tổng thể, các quy tắc và cam kết, được thể hiện chính thức bởi người kiểm soát thông tin nhận dạng cá nhân (PII) (3.8) liên quan đến việc xử lý PII (3.7) trong một bối cảnh cụ thể.

3.15

Lựa chọn quyền riêng tư (Privacy preference)

Các lựa chọn cụ thể được thực hiện bởi chủ thể thông tin nhận dạng cá nhân (PII) (3.9) về cách PII của họ (3.7) nên được xử lý cho một mục đích cụ thể.

3.16

Nguyên tắc quyền riêng tư (Privacy principle)

Là giá trị chung chi phối việc bảo vệ quyền riêng tư đối với thông tin nhận dạng cá nhân (PII) (3.7) khi được xử lý trong các hệ thống công nghệ thông tin và truyền thông

3.17

Rủi ro về quyền riêng tư (Privacy risk)

Là tác động của sự không chắc chắn đối với quyền riêng tư.

Chú thích 1: Trong ISO Guide 73 (Tiêu chuẩn này đã được thu hồi) và ISO 31000, rủi ro được định nghĩa là “tác động của sự không chắc chắn đối với các mục tiêu”.

Chú thích 2: Sự không chắc chắn là trạng thái, dù chỉ là một phần, của sự thiếu thông tin liên quan đến, sự hiểu biết hoặc kiến thức về, một sự kiện, hậu quả của nó hoặc khả năng xảy ra của nó.

3.18

Đánh giá tác động quyền riêng tư (Privacy impact assessment)

Là quá trình tổng thể nhằm xác định, phân tích, đánh giá, tham vấn, trao đổi thông tin và lập kế hoạch xử lý các tác động tiềm ẩn đối với quyền riêng tư liên quan đến việc xử lý thông tin nhận dạng cá nhân (PII) (3.7), được thực hiện trong khuôn khổ quản lý rủi ro chung của tổ chức.

3.19

Yêu cầu bảo vệ quyền riêng tư (Privacy safeguarding requirement)

Là yêu cầu mà tổ chức cần cân nhắc khi xử lý thông tin nhận dạng cá nhân (PII) (3.7), nhằm bảo vệ quyền riêng tư của các thông tin này.

3.20

Bên liên quan quyền riêng tư (Privacy stakeholder)

Là cá nhân hoặc pháp nhân, cơ quan nhà nước, tổ chức, hoặc bất kỳ chủ thể nào khác có thể tác động đến, bị tác động bởi, hoặc tự nhận thấy mình bị tác động bởi các quyết định hoặc hoạt động liên quan đến việc xử lý thông tin nhận dạng cá nhân (PII) (3.7).

3.21

Việc xử lý thông tin nhận dạng cá nhân (Processing of PII)

Là một hoạt động hoặc một tập hợp các hoạt động được thực hiện đối với thông tin nhận dạng cá nhân (PII) (3.7).

Chú thích 1: Các hoạt động xử lý PII có thể bao gồm, nhưng không chỉ giới hạn ở, việc thu thập, lưu trữ, chỉnh

sửa, truy cập, tra cứu, công bố, ẩn danh hóa (3.2), giả danh hóa (3.22), xóa bỏ hoặc tiêu hủy PII, cũng như việc chia sẻ hoặc cung cấp PII dưới các hình thức khác.

3.22

Giả danh hóa (Pseudonymization)

Là quá trình được áp dụng đối với thông tin nhận dạng cá nhân (PII) (3.7), trong đó thông tin định danh được thay thế bằng một bí danh.

Chú thích 1: Giả danh hóa có thể được thực hiện bởi chính chủ thể PII (3.9) hoặc bởi bên kiểm soát PII (3.8). Việc giả danh hóa cho phép chủ thể PII sử dụng hoặc truy cập một tài nguyên hay dịch vụ một cách nhất quán mà không cần tiết lộ danh tính của mình cho tài nguyên hoặc dịch vụ đó (hoặc giữa các dịch vụ), đồng thời vẫn bảo đảm khả năng truy cứu trách nhiệm đối với việc sử dụng này.

Chú thích 2: Giả danh hóa không loại trừ khả năng tồn tại một nhóm giới hạn các bên liên quan về quyền riêng tư (3.20), ngoài bên kiểm soát PII của dữ liệu đã được giả danh hóa, vẫn có thể xác định được danh tính của chủ thể PII dựa trên bí danh và các dữ liệu được liên kết với bí danh đó.

3.23

Thông tin nhận dạng cá nhân nhạy cảm (Sensitive PII)

Loại thông tin nhận dạng cá nhân (PII) (3.7), có tính chất nhạy cảm, chẳng hạn như những thông tin liên quan đến lĩnh vực riêng tư nhất của chủ thể PII (3.9), hoặc có thể có tác động đáng kể đến chủ thể PII.

Chú thích 1: Tại một số quốc gia hoặc trong những bối cảnh cụ thể, thông tin nhận dạng cá nhân nhạy cảm được xác định dựa trên bản chất của PII và có thể bao gồm các PII làm lộ nguồn gốc chủng tộc, quan điểm chính trị, tín ngưỡng tôn giáo hoặc các niềm tin khác, dữ liệu cá nhân về sức khỏe, đời sống tình dục hoặc tiền án, tiền sự, cũng như các PII khác có thể được coi là nhạy cảm.

3.24

Bên thứ 3 (Third party)

Là bên liên quan về quyền riêng tư (3.20) không bao gồm chủ thể thông tin nhận dạng cá nhân (PII) (3.9), bên kiểm soát PII (3.8), bên xử lý PII (3.10), cũng như các cá nhân được ủy quyền xử lý dữ liệu dưới sự chỉ đạo trực tiếp của bên kiểm soát PII hoặc bên xử lý PII.

4 Ký hiệu và các thuật ngữ viết tắt

ICT: Công nghệ thông tin và truyền thông

PET: Công nghệ tăng cường quyền riêng tư

PII: Thông tin nhận dạng cá nhân

5 Các yếu tố cơ bản của khung quyền riêng tư

5.1 Tổng quan về khung quyền riêng tư

Các thành phần sau đây liên quan đến quyền riêng tư và việc xử lý thông tin nhận dạng cá nhân (PII) trong các hệ thống công nghệ thông tin và truyền thông, và tạo thành khung quyền riêng tư được trình bày trong tiêu chuẩn này.

-— Các chủ thể và vai trò;

— Các mối tương tác;

— Nhận diện thông tin nhận dạng cá nhân (PII);

— Các yêu cầu bảo vệ quyền riêng tư;

— Các chính sách quyền riêng tư;

— Các biện pháp kiểm soát quyền riêng tư.

Để xây dựng khung quyền riêng tư này, các khái niệm, định nghĩa và khuyến nghị từ những nguồn chính thức khác đã được xem xét và tham chiếu. Các nguồn này được liệt kê tại Tài liệu tham khảo [3].

CHÚ THÍCH: Nhằm tạo thuận lợi cho việc sử dụng ISO/IEC 27000 và các tiêu chuẩn quốc tế liên quan đến hệ thống quản lý an toàn thông tin (ISMS) [4]–[25] trong bối cảnh cụ thể của quyền riêng tư, cũng như để tích hợp các khái niệm về quyền riêng tư vào bối cảnh ISO/IEC 27000, Bảng A.1 trình bày sự tương ứng giữa các khái niệm trong các tài liệu tham khảo từ [4] đến [25] với các khái niệm được sử dụng trong tài liệu này.

5.2 Các chủ thể và vai trò

5.2.1 Quy định chung

Đối với tiêu chuẩn này, việc xác định các chủ thể tham gia vào quá trình xử lý thông tin nhận dạng cá nhân (PII) là rất quan trọng. Có bốn loại chủ thể có thể tham gia vào việc xử lý PII, bao gồm: chủ thể PII, bên kiểm soát PII, bên xử lý PII và bên thứ ba.

5.2.2 Chủ thể PII

Chủ thể PII cung cấp thông tin nhận dạng cá nhân của mình để các bên kiểm soát PII và bên xử lý PII thực hiện việc xử lý; đồng thời, trong trường hợp pháp luật hiện hành không có quy định khác, họ đưa ra sự đồng ý và xác định các lựa chọn quyền riêng tư của mình đối với cách thức PII được xử lý.

Chủ thể PII có thể là, chẳng hạn, một nhân viên được quản lý trong hệ thống nhân sự của doanh nghiệp, một người tiêu dùng được nêu trong báo cáo tín dụng, hoặc một bệnh nhân được ghi nhận trong hồ sơ y tế điện tử. Thể nhân liên quan không nhất thiết phải được xác định trực tiếp bằng tên thì mới được coi là chủ thể PII. Trường hợp thể nhân mà PII gắn với có thể được xác định một cách gián tiếp (ví dụ thông qua mã tài khoản, số an sinh xã hội, hoặc thông qua sự kết hợp của các thuộc tính sẵn có), thì người đó vẫn được coi là chủ thể PII đối với tập dữ liệu PII tương ứng.

5.2.3 Bên kiểm soát PII

Bên kiểm soát PII quyết định lý do (mục đích) và cách thức (phương tiện) mà việc xử lý PII được thực hiện. Bên kiểm soát PII cần bảo đảm việc tuân thủ các nguyên tắc bảo vệ quyền riêng tư trong khung này trong suốt quá trình xử lý PII thuộc phạm vi kiểm soát của mình (ví dụ thông qua việc triển khai các biện pháp kiểm soát quyền riêng tư cần thiết).

Có thể tồn tại nhiều hơn một bên kiểm soát PII đối với cùng một tập PII hoặc cùng một tập các hoạt động xử lý PII (phục vụ cho cùng hoặc cho các mục đích hợp pháp khác nhau). Trong trường hợp đó, các bên kiểm soát PII khác nhau phải phối hợp với nhau và thực hiện các sắp xếp cần thiết nhằm bảo đảm các nguyên tắc bảo vệ quyền riêng tư được tuân thủ trong quá trình xử lý PII.

Bên kiểm soát PII cũng có thể quyết định giao toàn bộ hoặc một phần các hoạt động xử lý cho một bên liên quan về quyền riêng tư khác thực hiện thay mặt mình. Bên cạnh đó, bên kiểm soát PII được kỳ vọng sẽ đánh giá cẩn trọng việc có hay không xử lý PII nhạy cảm,

đồng thời triển khai các biện pháp bảo vệ quyền riêng tư và an ninh phù hợp, hợp lý, cũng như xem xét các tác động bất lợi tiềm ẩn đối với chủ thể PII được xác định thông qua quá trình đánh giá rủi ro về quyền riêng tư.

Chú thích: Các yêu cầu pháp lý có thể được áp dụng

5.2.4 Bên xử lý PII

Bên xử lý PII thực hiện việc xử lý thông tin nhận dạng cá nhân thay mặt cho bên kiểm soát PII, làm việc theo sự ủy quyền hoặc theo hướng dẫn của bên kiểm soát PII, tuân thủ các yêu cầu về quyền riêng tư đã được đặt ra và áp dụng các biện pháp kiểm soát quyền riêng tư tương ứng.

CHÚ THÍCH: Ở một số khu vực pháp lý, bên xử lý PII có thể bị ràng buộc bởi hợp đồng.

5.2.5 Bên thứ ba

Bên thứ ba có thể nhận thông tin nhận dạng cá nhân từ bên kiểm soát PII hoặc bên xử lý PII. Bên thứ ba không thực hiện việc xử lý PII thay mặt cho bên kiểm soát PII. Thông thường, sau khi nhận được PII liên quan, bên thứ ba sẽ trở thành một bên kiểm soát PII độc lập đối với các thông tin đó.

5.3 Các mối tương tác

Các chủ thể được xác định tại 5.2 có thể tương tác với nhau theo nhiều cách khác nhau. Xét về các luồng thông tin nhận dạng cá nhân (PII) có thể xảy ra giữa chủ thể PII, bên kiểm soát PII và bên xử lý PII, có thể nhận diện các kịch bản sau:
a) chủ thể PII cung cấp PII cho bên kiểm soát PII (ví dụ khi đăng ký sử dụng một dịch vụ do bên kiểm soát PII cung cấp);
b) bên kiểm soát PII cung cấp PII cho bên xử lý PII để bên này xử lý PII thay mặt cho bên kiểm soát PII (ví dụ trong khuôn khổ một thỏa thuận thuê ngoài);
c) chủ thể PII cung cấp PII cho bên xử lý PII, bên này xử lý PII thay mặt cho bên kiểm soát PII;
d) bên kiểm soát PII cung cấp cho chủ thể PII các thông tin PII liên quan đến chính chủ thể PII đó (ví dụ theo yêu cầu của chủ thể PII);
e) bên xử lý PII cung cấp PII cho chủ thể PII (ví dụ theo chỉ đạo của bên kiểm soát PII);
f) bên xử lý PII cung cấp PII cho bên kiểm soát PII (ví dụ sau khi đã thực hiện xong dịch vụ mà mình được giao).
Vai trò của chủ thể PII, bên kiểm soát PII, bên xử lý PII và bên thứ ba trong các kịch bản này được minh họa tại Bảng 1.

Cần phân biệt rõ giữa bên xử lý PII và bên thứ ba, bởi vì quyền kiểm soát pháp lý đối với PII vẫn thuộc về bên kiểm soát PII ban đầu khi PII được chuyển cho bên xử lý PII; trong khi đó, bên thứ ba có thể trở thành một bên kiểm soát PII độc lập sau khi nhận được PII liên quan. Chẳng hạn, trong trường hợp một bên thứ ba tự mình quyết định chuyển PII mà họ đã nhận từ bên kiểm soát PII sang cho một bên khác, thì bên thứ ba đó đang hành động với tư cách là bên kiểm soát PII độc lập và vì vậy sẽ không còn được coi là bên thứ ba nữa.

Xét về các luồng thông tin nhận dạng cá nhân (PII) có thể xảy ra giữa, một bên là các bên kiểm soát PII và bên xử lý PII, và bên kia là các bên thứ ba, có thể nhận diện các kịch bản sau:

g) bên kiểm soát PII cung cấp PII cho bên thứ ba (ví dụ trong khuôn khổ một thỏa thuận kinh doanh); và

h) bên xử lý PII cung cấp PII cho bên thứ ba (ví dụ theo chỉ đạo của bên kiểm soát PII).

Vai trò của bên kiểm soát PII và bên thứ ba trong các kịch bản này cũng được minh họa tại Bảng 1.

Bảng 1 — Các luồng thông tin nhận dạng cá nhân có thể xảy ra giữa chủ thể PII, bên kiểm soát PII, bên xử lý PII và bên thứ ba, cùng với vai trò của các bên

	Chủ thể PII	**Bên kiểm soát PII**	**Bên xử lý PII**	**Bên thứ ba**
Kịch bản a)	Nhà cung cấp PII	Bên nhận PII	—	—
Kịch bản b)	—	Nhà cung cấp PII	Bên nhận PII	—
Kịch bản c)	Nhà cung cấp PII	—	Bên nhận PII	—
Kịch bản d)	Bên nhận PII	Nhà cung cấp PII	—	—
Kịch bản e)	Bên nhận PII	—	Nhà cung cấp PII	—
Kịch bản f)	—	Bên nhận PII	Nhà cung cấp PII	—
Kịch bản g)	—	Nhà cung cấp PII	—	Bên nhận PII
Kịch bản h)	—	—	Nhà cung cấp PII	Bên nhận PII

5.4 Xác định thông tin nhận dạng cá nhân (PII)

5.4.1 Quy định chung

Để xác định liệu một thể nhân có nên được coi là có thể xác định được hay không, cần xem xét nhiều yếu tố khác nhau. Đặc biệt, cần tính đến tất cả các phương thức có thể được sử dụng một cách hợp lý bởi bên liên quan về quyền riêng tư đang nắm giữ dữ liệu, hoặc bởi bất kỳ bên nào khác, nhằm xác định danh tính của thể nhân đó.

Các hệ thống công nghệ thông tin và truyền thông cần hỗ trợ các cơ chế giúp chủ thể PII biết được các thông tin PII liên quan đến mình, đồng thời cho phép thể nhân đó thực hiện các biện pháp kiểm soát phù hợp đối với việc chia sẻ các thông tin này. Các Điều từ 5.4.2 đến 5.4.8 cung cấp thêm hướng dẫn nhằm làm rõ cách xác định liệu một chủ thể PII có nên được coi là có thể xác định được hay không.

5.4.2 Các mã định danh

Trong một số trường hợp, việc xác định chủ thể PII rất rõ ràng, chẳng hạn khi thông tin chứa hoặc gắn với một định danh dùng để gọi tên hoặc liên lạc với chủ thể PII. Thông tin có thể được coi là thông tin nhận dạng cá nhân (PII) trong ít nhất các trường hợp sau:

— khi thông tin chứa hoặc gắn với một định danh chỉ trực tiếp tới một thể nhân (ví dụ số an sinh xã hội);
— khi thông tin chứa hoặc gắn với một định danh có thể liên hệ tới một thể nhân (ví dụ số hộ chiếu, số tài khoản);
— khi thông tin chứa hoặc gắn với một định danh có thể dùng để liên lạc với một thể nhân đã được xác định (ví dụ vị trí địa lý chính xác, số điện thoại); hoặc
— khi thông tin có chứa tham chiếu liên kết dữ liệu với bất kỳ định danh nào nêu trên.

5.4.3 Các đặc điểm phân biệt khác

Thông tin không nhất thiết phải gắn với một định danh thì mới được coi là PII. Thông tin cũng được xem là PII nếu nó chứa hoặc gắn với một đặc điểm giúp phân biệt một thể nhân với các thể nhân khác (ví dụ dữ liệu sinh trắc học).
Bất kỳ thuộc tính nào mang một giá trị có thể xác định duy nhất một chủ thể PII đều được coi là một đặc điểm phân biệt. Việc một đặc điểm cụ thể có giúp phân biệt một thể nhân với các thể nhân khác hay không còn phụ thuộc vào bối cảnh sử dụng. Chẳng hạn, họ của một người có thể chưa đủ để xác định người đó trên phạm vi toàn cầu, nhưng thường lại đủ để phân biệt người đó trong phạm vi một doanh nghiệp.

Ngoài ra, trong một số trường hợp, người ta vẫn có thể xác định được một thể nhân ngay cả khi không có thuộc tính riêng lẻ nào đủ để xác định duy nhất thể nhân đó. Khi kết hợp nhiều thuộc tính lại với nhau, các thuộc tính này có thể giúp phân biệt thể nhân đó với những thể nhân khác. Việc xác định một cá nhân dựa trên sự kết hợp các thuộc tính cũng phụ thuộc vào từng lĩnh vực cụ thể.
Chẳng hạn, khi kết hợp các thuộc tính “nữ”, “45 tuổi” và “luật sư”, người ta có thể xác định được một thể nhân trong phạm vi một doanh nghiệp cụ thể; tuy nhiên, sự kết hợp này thường không đủ để xác định thể nhân đó ngoài phạm vi doanh nghiệp.
Bảng 2 đưa ra một số ví dụ về các thuộc tính có thể được coi là PII tùy theo từng lĩnh vực. Các ví dụ này mang tính minh họa.

Bảng 2 — Ví dụ về các thuộc tính có thể dùng để xác định thể nhân

Ví dụ
Tuổi hoặc các nhu cầu đặc biệt của thể nhân dễ bị tổn thương
Các cáo buộc về hành vi phạm tội
Mọi thông tin được thu thập trong quá trình cung cấp dịch vụ y tế
Số tài khoản ngân hàng hoặc số thẻ tín dụng
Dữ liệu định danh sinh trắc học
Sao kê thẻ tín dụng
Các bản án hình sự hoặc hành vi phạm tội đã thực hiện
Báo cáo điều tra hình sự
Mã số khách hàng
Ngày, tháng, năm sinh
Thông tin chẩn đoán về sức khỏe
Tình trạng khuyết tật
Hóa đơn, chi phí khám chữa bệnh
Tiền lương của người lao động và hồ sơ nhân sự
Hồ sơ tài chính
Giới tính
Vị trí GPS
Lộ trình, lịch sử di chuyển theo GPS
Địa chỉ nơi cư trú
Địa chỉ IP
Vị trí được xác định từ hệ thống viễn thông
Tiền sử bệnh lý
Họ và tên

Các mã định danh quốc gia (ví dụ số hộ chiếu)
Địa chỉ email cá nhân
Số định danh cá nhân (PIN) hoặc mật khẩu
Sở thích cá nhân được suy ra từ việc theo dõi sử dụng các trang web
Hồ sơ cá nhân hoặc hành vi
Số điện thoại cá nhân
Hình ảnh hoặc video có thể xác định danh tính của thể nhân
Sở thích về sản phẩm và dịch vụ
Nguồn gốc chủng tộc hoặc dân tộc
Niềm tin tôn giáo hoặc triết lý sống
Xu hướng tính dục
Tư cách thành viên công đoàn
Hóa đơn tiện ích

5.4.4 Thông tin đang hoặc có thể liên kết với chủ thể PII

Nếu thông tin được đề cập không xác định được chủ thể thông tin nhận dạng cá nhân (PII), cần phải xác định xem thông tin đó có liên quan hoặc có thể liên quan đến danh tính của một thể nhân cụ thể hay không.

Khi mối liên kết với một thể nhân có thể xác định được, cần quyết định xem thông tin đó có phản ánh điều gì về thể nhân này hay không, ví dụ như đặc điểm hoặc hành vi của họ. Các ví dụ bao gồm hồ sơ y tế, hồ sơ tài chính, hoặc sở thích cá nhân được suy ra từ việc theo dõi hoạt động trên Internet. Ngoài ra, những thông tin đơn giản về một thể nhân, như tuổi hay giới tính, cũng có thể khiến thông tin liên kết đó được coi là PII.

Bất kể trường hợp nào, nếu có thể xác định được mối liên hệ với một thể nhân, thông tin đó phải được coi và xử lý như PII.

5.4.5 Dữ liệu giả danh

Để hạn chế khả năng xác định chủ thể PII, các bên kiểm soát và xử lý PII có thể thay thế thông tin định danh bằng bí danh. Người cung cấp PII thường thực hiện việc thay thế này trước khi chuyển PII cho người nhận PII, đặc biệt trong các tình huống a, b, c, g và h được liệt kê trong Bảng 1.

Một số quy trình kinh doanh yêu cầu các bên xử lý được chỉ định thực hiện việc thay thế và quản lý bảng hoặc hàm phân bổ bí danh. Việc này thường xảy ra khi dữ liệu nhạy cảm cần được xử lý bởi những người liên quan về quyền riêng tư nhưng không phải là người thu thập dữ liệu ban đầu.

Việc thay thế này được gọi là giả danh, khi thỏa hai điều kiện sau:

a) Các thông tin còn lại gắn với bí danh không đủ để xác định chủ thể PII mà chúng liên quan; và

b) Việc gán bí danh được thực hiện sao cho các bên liên quan về quyền riêng tư không thể phục hồi danh tính gốc, trừ những người trực tiếp thực hiện việc gán bí danh.

Việc giả danh vẫn giữ khả năng liên kết. Các dữ liệu khác nhau gắn với cùng một bí danh có thể được liên kết với nhau. Càng nhiều dữ liệu gắn với cùng một bí danh thì nguy cơ vi phạm điều kiện a) càng cao. Hơn nữa, nhóm thể nhân liên quan đến một tập dữ liệu giả danh càng nhỏ, khả năng xác định được chủ thể PII càng lớn. Khi xác định liệu thông tin có liên quan đến một thể nhân có thể xác định được hay không, cần xem xét các thuộc tính có trong thông tin đó cũng như các thuộc tính có thể dễ dàng liên kết với thông tin này (ví dụ: thông qua công cụ tìm kiếm hoặc đối chiếu với các cơ sở dữ liệu khác).

Giả danh khác với ẩn danh. Quá trình ẩn danh cũng đáp ứng các điều kiện a) và b) nêu trên, nhưng loại bỏ khả năng liên kết. Khi ẩn danh, người xử lý xóa bỏ thông tin định danh hoặc thay thế bằng bí danh và hủy bảng hoặc hàm gán bí danh. Vì vậy, dữ liệu sau khi ẩn danh không còn là PII.

5.4.6 Siêu dữ liệu (Metadata)

Hệ thống ICT có thể lưu trữ PII mà người dùng hệ thống không nhìn thấy trực tiếp (tức là chính chủ thể PII không thấy). Ví dụ: tên của chủ thể PII được lưu dưới dạng siêu dữ liệu trong thuộc tính của tài liệu, hoặc các nhận xét, thay đổi theo dõi được lưu dưới dạng siêu dữ liệu trong tài liệu soạn thảo văn bản.
Nếu chủ thể PII biết rằng dữ liệu của họ tồn tại hoặc đang được xử lý cho mục đích này, họ có thể không muốn PII được xử lý theo cách đó hoặc bị chia sẻ công khai.

5.4.7 PII không được yêu cầu

Hệ thống ICT cũng có thể lưu trữ PII mà các bên kiểm soát hoặc xử lý PII không yêu cầu (tức là PII được thu thập một cách tình cờ). Ví dụ: chủ thể PII có thể cung cấp PII cho bên kiểm soát PII mà bên này không yêu cầu (ví dụ: thông tin bổ sung gửi qua biểu mẫu phản hồi ẩn danh trên website).
Nguy cơ thu thập PII không được yêu cầu có thể giảm thiểu bằng cách áp dụng các biện pháp bảo vệ quyền riêng tư ngay từ giai đoạn thiết kế hệ thống (còn được gọi là khái niệm “privacy by design”).

5.4.8 PII nhạy cảm

Tính nhạy cảm bao gồm tất cả PII từ đó có thể suy ra PII nhạy cảm. Ví dụ, đơn thuốc có thể tiết lộ thông tin chi tiết về sức khỏe của chủ thể PII.
Ngay cả khi PII không chứa thông tin trực tiếp về xu hướng tính dục hoặc tình trạng sức khỏe của chủ thể, nếu PII đó có thể dùng để suy ra những thông tin này, thì PII vẫn được coi là nhạy cảm.
Trong phạm vi tiêu chuẩn này, PII sẽ được xem là PII nhạy cảm nếu việc suy luận thông tin nhạy cảm và nhận diện chủ thể PII là khả thi hợp lý.

GHI CHÚ 1: Ở một số khu vực pháp lý, PII nhạy cảm được pháp luật quy định rõ ràng. Ví dụ bao gồm thông tin tiết lộ chủng tộc, nguồn gốc dân tộc, niềm tin tôn giáo hoặc triết lý sống, quan điểm chính trị, tư cách thành viên công đoàn, lối sống hoặc xu hướng tính dục, và tình trạng sức khỏe thể chất hoặc tinh thần của chủ thể PII.
Ở những khu vực khác, PII nhạy cảm có thể bao gồm thông tin dễ dẫn đến đánh cắp danh tính hoặc gây thiệt hại tài chính đáng kể cho thể nhân (ví dụ: số thẻ tín dụng, thông tin tài khoản ngân hàng, hoặc các mã định danh do chính phủ cấp như số hộ chiếu, số an sinh xã hội, số bằng lái xe), cũng như thông tin có thể xác định vị trí thực tế của chủ thể PII theo thời gian thực.

Việc xử lý PII nhạy cảm đòi hỏi các biện pháp phòng ngừa đặc biệt.

GHI CHÚ 2: Ở một số khu vực pháp lý, việc xử lý PII nhạy cảm có thể bị pháp luật cấm, ngay cả khi chủ thể PII đã đồng ý tham gia (opt-in). Một số khu vực pháp lý có thể yêu cầu thực hiện các biện pháp kiểm soát cụ thể khi xử lý một số loại PII nhạy cảm nhất định (ví dụ: yêu cầu mã hóa PII y tế khi truyền qua mạng công cộng).

5.5 Yêu cầu bảo vệ quyền riêng tư

5.5.1 Quy định chung

Các tổ chức có động lực để bảo vệ PII vì nhiều lý do: bảo vệ quyền riêng tư của chủ thể PII, tuân thủ các yêu cầu pháp lý và quy định, thực hiện trách nhiệm xã hội của doanh nghiệp và tăng cường niềm tin của người tiêu dùng. Mục đích của điều khoản này là cung cấp cái nhìn

tổng quan về các yếu tố khác nhau có thể ảnh hưởng đến các yêu cầu bảo vệ quyền riêng tư, phù hợp với một tổ chức hoặc bên liên quan về quyền riêng tư khi xử lý PII.

Các yêu cầu bảo vệ quyền riêng tư có thể liên quan đến nhiều khía cạnh khác nhau của việc xử lý PII, ví dụ: việc thu thập và lưu giữ PII, chuyển giao PII cho bên thứ ba, mối quan hệ hợp đồng giữa các bên kiểm soát và xử lý PII, cũng như việc chuyển giao PII ra quốc tế.

Các yêu cầu bảo vệ quyền riêng tư cũng có thể khác nhau về mức độ chi tiết. Chúng có thể rất tổng quát, ví dụ: liệt kê các nguyên tắc bảo vệ quyền riêng tư ở mức cao mà tổ chức cần xem xét khi xử lý PII. Tuy nhiên, các yêu cầu này cũng có thể đưa ra các hạn chế rất cụ thể đối với việc xử lý một số loại PII nhất định, hoặc yêu cầu thực hiện các biện pháp kiểm soát quyền riêng tư cụ thể.

Việc thiết kế bất kỳ hệ thống ICT nào có liên quan đến xử lý PII nên được tiến hành sau khi xác định các yêu cầu bảo vệ quyền riêng tư liên quan. Các tác động về quyền riêng tư của những hệ thống ICT mới hoặc được sửa đổi đáng kể, liên quan đến xử lý PII, cần được giải quyết trước khi triển khai các hệ thống này.

Các tổ chức thường thực hiện các hoạt động quản lý rủi ro tổng thể và xây dựng hồ sơ rủi ro liên quan đến hệ thống ICT của mình.

Quản lý rủi ro được định nghĩa là các hoạt động phối hợp nhằm định hướng và kiểm soát tổ chức liên quan đến rủi ro (xem ISO Guide 73(tiêu chuẩn này đã được thu hồi)). Quá trình quản lý rủi ro về quyền riêng tư bao gồm các quy trình sau:

— Xác định bối cảnh, bằng cách hiểu tổ chức (ví dụ: việc xử lý PII, trách nhiệm), môi trường kỹ thuật và các yếu tố ảnh hưởng đến quản lý rủi ro quyền riêng tư (ví dụ: các yếu tố pháp lý và quy định, yếu tố hợp đồng, yếu tố kinh doanh và các yếu tố khác)

— Đánh giá rủi ro, bằng cách xác định, phân tích và đánh giá các rủi ro đối với chủ thể PII (các rủi ro có thể gây ảnh hưởng bất lợi đến họ)

— Xử lý rủi ro, bằng cách xác định các yêu cầu bảo vệ quyền riêng tư, xác định và triển khai các biện pháp kiểm soát quyền riêng tư để tránh hoặc giảm thiểu các rủi ro đối với chủ thể PII

— Truyền thông và tham vấn, bằng cách thu thập thông tin từ các bên quan tâm, đạt được sự đồng thuận về từng quy trình quản lý rủi ro, và thông báo cho chủ thể PII cũng như trao đổi về các rủi ro và biện pháp kiểm soát

— Giám sát và xem xét, bằng cách theo dõi các rủi ro và biện pháp kiểm soát, đồng thời cải thiện quy trình

Một kết quả có thể tạo ra là đánh giá tác động quyền riêng tư. Đây là phần của quản lý rủi ro giúp tổ chức đảm bảo tuân thủ các quy định về quyền riêng tư và bảo vệ dữ liệu, đồng thời xem xét ảnh hưởng về quyền riêng tư của các chương trình hoặc hoạt động mới, hoặc những chương trình/hoạt động đã được thay đổi đáng kể. Đánh giá tác động quyền riêng tư nên được thực hiện trong khuôn khổ quản lý rủi ro tổng thể của tổ chức.

Hình 1 — Các yếu tố ảnh hưởng đến quản lý rủi ro quyền riêng tư

Các yêu cầu bảo vệ quyền riêng tư được xác định như một phần của quy trình quản lý rủi ro quyền riêng tư tổng thể, chịu ảnh hưởng bởi các yếu tố sau (như minh họa trong Hình 1 ở trên và mô tả dưới đây):

— Các yếu tố pháp lý và quy định liên quan đến việc bảo vệ quyền riêng tư của thể nhân và bảo vệ PII của họ

— Các yếu tố hợp đồng, chẳng hạn như các thỏa thuận giữa nhiều bên khác nhau, chính sách công ty và các quy tắc ràng buộc trong doanh nghiệp

— Các yếu tố kinh doanh, được xác định trước bởi một ứng dụng kinh doanh cụ thể hoặc trong bối cảnh sử dụng cụ thể

— Các yếu tố khác có thể ảnh hưởng đến thiết kế hệ thống ICT và các yêu cầu bảo vệ quyền riêng tư liên quan

5.5.2 Các yếu tố pháp lý và quy định

Các yêu cầu bảo vệ quyền riêng tư thường được thể hiện trong:

(1) Luật pháp quốc tế, quốc gia và địa phương,

(2) Các quy định,

(3) Các quyết định tư pháp, hoặc

(4) Các thỏa thuận đã thương lượng với hội đồng lao động hoặc các tổ chức công đoàn khác.

Một số ví dụ về luật pháp quốc gia và địa phương bao gồm: luật bảo vệ dữ liệu, luật bảo vệ người tiêu dùng, luật thông báo vi phạm dữ liệu, luật lưu giữ dữ liệu và luật lao động. Luật pháp quốc tế liên quan cũng có thể chứa các quy định ảnh hưởng đến việc chuyển giao PII qua biên giới.

Các bên kiểm soát PII cần nhận biết tất cả các yêu cầu bảo vệ quyền riêng tư liên quan phát sinh từ các yếu tố pháp lý hoặc quy định. Để đạt được mục tiêu này, họ có thể phối hợp chặt chẽ với các chuyên gia pháp lý.

Trong nhiều khu vực pháp lý, bên kiểm soát PII sẽ là người chịu trách nhiệm cuối cùng trong việc đảm bảo tuân thủ, nhưng tất cả các bên tham gia xử lý PII cũng nên chủ động trong việc xác định các yêu cầu bảo vệ quyền riêng tư liên quan phát sinh từ các yếu tố pháp lý hoặc các yếu tố khác.

5.5.3 Các yếu tố hợp đồng

Các nghĩa vụ hợp đồng cũng có thể ảnh hưởng đến các yêu cầu bảo vệ quyền riêng tư. Những nghĩa vụ này có thể xuất phát từ các thỏa thuận giữa nhiều bên khác nhau, chẳng hạn như các bên xử lý PII, các bên kiểm soát PII và bên thứ ba.

Ví dụ, một bên liên quan về quyền riêng tư có thể yêu cầu bên thứ ba sử dụng các biện pháp kiểm soát quyền riêng tư cụ thể và đồng ý thực hiện các yêu cầu về hủy bỏ PII trước khi PII được chuyển giao cho họ.

Các yêu cầu bảo vệ quyền riêng tư cũng có thể phát sinh từ chính sách công ty và các quy tắc ràng buộc trong doanh nghiệp mà bên liên quan về quyền riêng tư đặt ra cho chính mình, ví dụ để bảo vệ thương hiệu khỏi những ảnh hưởng tiêu cực nếu xảy ra sự cố vi phạm quyền riêng tư.

Về nguyên tắc, bất kỳ bên nào có quyền truy cập PII đều nên được thông báo về các nghĩa vụ của mình bởi các bên kiểm soát PII một cách chính thức, ví dụ thông qua việc ký kết các thỏa thuận với bên thứ ba. Những thỏa thuận này thường chứa một số yêu cầu bảo vệ quyền riêng tư mà người nhận PII sẽ phải xem xét và thực hiện.

GHI CHÚ: Ở một số khu vực pháp lý, các cơ quan quốc gia và khu vực có thể thiết lập các công cụ pháp lý và hợp đồng để cho phép chuyển giao PII cho bên thứ ba.

5.5.4 Các yếu tố kinh doanh

Các yêu cầu bảo vệ quyền riêng tư cũng có thể bị ảnh hưởng bởi các yếu tố kinh doanh, bao gồm các đặc điểm cụ thể của ứng dụng dự kiến hoặc bối cảnh sử dụng của nó. Các yếu tố kinh doanh có thể rất khác nhau tùy thuộc vào loại bên liên quan về quyền riêng tư và loại hình kinh doanh.
Ví dụ, các yếu tố này có thể liên quan đến lĩnh vực mà tổ chức hoạt động (ví dụ: hướng dẫn ngành, quy tắc ứng xử, thực tiễn tốt nhất, tiêu chuẩn) hoặc bản chất mô hình kinh doanh của tổ chức (ví dụ: dịch vụ trực tuyến 24/7, dịch vụ chia sẻ thông tin, ứng dụng ngân hàng).

Nhiều yếu tố kinh doanh không tác động trực tiếp đến các yêu cầu bảo vệ quyền riêng tư. Tuy nhiên, mục đích sử dụng PII dự kiến có thể ảnh hưởng đến việc triển khai chính sách quyền riêng tư của tổ chức cũng như lựa chọn các biện pháp kiểm soát quyền riêng tư.
Tổ chức không nên thay đổi các nguyên tắc quyền riêng tư mà mình tuân thủ chỉ vì các yếu tố kinh doanh. Ví dụ, việc cung cấp một dịch vụ nhất định có thể yêu cầu nhà cung cấp dịch vụ thu thập thêm PII hoặc cho phép nhiều nhân viên hơn xử lý một số loại PII nhất định.
Tuy nhiên, bên kiểm soát PII đã cam kết tuân thủ các nguyên tắc trong khuôn khổ này vẫn cần đánh giá kỹ loại PII nào thật sự cần thiết để cung cấp dịch vụ (nguyên tắc hạn chế thu thập) và giới hạn việc xử lý PII của nhân viên chỉ trong phạm vi cần thiết để thực hiện nhiệm vụ của họ (nguyên tắc tối thiểu hóa dữ liệu).

5.5.5 Các yếu tố khác

Yếu tố quan trọng nhất mà các tổ chức cần xem xét khi xác định các yêu cầu bảo vệ quyền riêng tư là sở thích về quyền riêng tư của chủ thể PII. Xu hướng cá nhân của một thể nhân đối với quyền riêng tư và những rủi ro mà họ quan tâm có thể phụ thuộc vào nhiều yếu tố, bao gồm: hiểu biết của thể nhân về công nghệ sử dụng, nền tảng của họ, thông tin được cung cấp, mục đích của giao dịch, kinh nghiệm trước đây của thể nhân, và các yếu tố tâm lý – xã hội.

Các nhà thiết kế hệ thống ICT nên cố gắng nắm bắt những lo ngại về quyền riêng tư có thể có của chủ thể thông tin cá nhân PII và hiểu rõ các loại PII sẽ được xử lý qua hệ thống của họ. Giống như nhà phát triển hệ thống hoặc nhà cung cấp ứng dụng/dịch vụ nghiên cứu các nhóm khách hàng mục tiêu về kỳ vọng sử dụng cũng như nhu cầu và mong muốn của họ, việc cố gắng hiểu các kỳ vọng và sở thích về quyền riêng tư của các thể nhân liên quan là rất quan trọng. Mặc dù không phải lúc nào các nhà thiết kế hệ thống ICT cũng có thể cung cấp cho chủ thể PII các lựa chọn phù hợp với sở thích quyền riêng tư của họ, nhưng đây vẫn là một yếu tố quan trọng cần xem xét trong thiết kế hệ thống.

Các ví dụ về sở thích về quyền riêng tư có thể bao gồm: mong muốn ẩn danh hoặc giả danh, khả năng hạn chế ai có thể truy cập vào PII cụ thể, hoặc khả năng hạn chế mục đích sử dụng PII. Trong phạm vi có thể, chủ thể PII nên được cung cấp lựa chọn về sở thích xử lý dữ liệu của họ, ví dụ như quyết định PII có được sử dụng cho các mục đích phụ như marketing hay không. Khả năng thể hiện các sở thích thân thiện với quyền riêng tư có thể được thực hiện thông qua giao diện người dùng đồ họa của hệ thống ICT. Giao diện này giúp chủ thể PII đưa ra lựa chọn bằng cách trình bày một tập hợp các tùy chọn đã định trước cho các sở thích quyền riêng tư phổ biến, sử dụng ngôn ngữ dễ hiểu. Việc triển khai giao diện người dùng có thể dựa trên các yếu tố như hộp kiểm hoặc menu thả xuống.

Ngoài các yếu tố đã liệt kê trong các điều khoản trước, vẫn còn các yếu tố khác có thể ảnh hưởng đến thiết kế hệ thống ICT và các yêu cầu bảo vệ quyền riêng tư liên quan. Ví dụ, các yêu cầu bảo vệ quyền riêng tư có thể bị ảnh hưởng bởi hệ thống kiểm soát nội bộ hoặc tiêu chuẩn kỹ thuật mà tổ chức đã áp dụng (ví dụ: một tiêu chuẩn tự nguyện, như tiêu chuẩn ISO).

5.5.6 Chính sách quyền riêng tư

Lãnh đạo cấp cao của tổ chức tham gia xử lý PII nên thiết lập một chính sách quyền riêng tư. Chính sách quyền riêng tư cần:
— Phù hợp với mục đích của tổ chức;
— Cung cấp khung để thiết lập các mục tiêu;
— Bao gồm cam kết tuân thủ các yêu cầu bảo vệ quyền riêng tư áp dụng;
— Bao gồm cam kết cải tiến liên tục;
— Được truyền đạt trong toàn tổ chức; và
— Có sẵn cho các bên quan tâm, tùy theo mức độ phù hợp.

Tổ chức nên ghi chép chính sách quyền riêng tư bằng văn bản. Trong trường hợp một tổ chức xử lý PII đóng vai trò là bên xử lý PII, các chính sách này có thể được xác định phần lớn bởi bên kiểm soát PII.
Chính sách quyền riêng tư nên được bổ sung bằng các quy tắc và nghĩa vụ chi tiết hơn của các bên liên quan về quyền riêng tư tham gia xử lý PII (ví dụ: các thủ tục dành cho bộ phận hoặc nhân viên cụ thể). Ngoài ra, các biện pháp kiểm soát được sử dụng để thực thi chính

sách quyền riêng tư trong bối cảnh cụ thể (ví dụ: kiểm soát truy cập, quy định thông báo, kiểm toán) cần được ghi chép rõ ràng.
Thuật ngữ "chính sách quyền riêng tư" thường được sử dụng để chỉ cả chính sách nội bộ và chính sách bên ngoài.

- Chính sách quyền riêng tư nội bộ ghi lại các mục tiêu, quy tắc, nghĩa vụ, hạn chế và/hoặc biện pháp kiểm soát mà tổ chức áp dụng để đáp ứng các yêu cầu bảo vệ quyền riêng tư liên quan đến việc xử lý PII của mình.
- Chính sách quyền riêng tư bên ngoài cung cấp cho các bên ngoài tổ chức thông báo về các thực tiễn quyền riêng tư của tổ chức, cũng như các thông tin liên quan khác như danh tính và địa chỉ chính thức của bên kiểm soát PII, các điểm liên hệ mà chủ thể PII có thể lấy thêm thông tin, v.v.

Trong khuôn khổ này, thuật ngữ "chính sách quyền riêng tư" được sử dụng để chỉ chính sách nội bộ của tổ chức, trong khi chính sách quyền riêng tư bên ngoài được gọi là thông báo.

5.5.7 Các biện pháp kiểm soát quyền riêng tư

Các tổ chức nên xác định và triển khai các biện pháp kiểm soát quyền riêng tư để đáp ứng các yêu cầu bảo vệ quyền riêng tư đã được xác định thông qua quy trình đánh giá và xử lý rủi ro quyền riêng tư. Ngoài ra, các biện pháp kiểm soát quyền riêng tư đã xác định và triển khai cần được ghi chép lại như một phần của đánh giá rủi ro quyền riêng tư của tổ chức.

Một số loại xử lý PII có thể cần các biện pháp kiểm soát cụ thể, mà nhu cầu chỉ trở nên rõ ràng sau khi một hoạt động dự kiến được phân tích cẩn thận. Việc đánh giá rủi ro quyền riêng tư có thể giúp tổ chức xác định các rủi ro cụ thể liên quan đến vi phạm quyền riêng tư trong một hoạt động dự kiến.
Các tổ chức nên phát triển các biện pháp kiểm soát quyền riêng tư như một phần của cách tiếp cận "quyền riêng tư ngay từ thiết kế" (privacy by design), nghĩa là tuân thủ quyền riêng tư cần được xem xét ngay từ giai đoạn thiết kế của các hệ thống xử lý PII, thay vì thêm vào ở giai đoạn sau. Đối với các biện pháp kiểm soát an ninh thông tin, cần lưu ý rằng không phải mọi xử lý PII đều yêu cầu cùng mức độ hoặc loại bảo vệ giống nhau. Các tổ chức nên phân biệt các hoạt động xử lý PII dựa trên các rủi ro cụ thể mà chúng mang lại, nhằm xác định biện pháp kiểm soát an ninh thông tin phù hợp cho từng trường hợp. Quản lý rủi ro là phương pháp trung tâm trong quy trình này, và việc xác định các biện pháp kiểm soát quyền riêng tư cũng nên là một phần không tách rời trong khuôn khổ quản lý an ninh thông tin của tổ chức.

6 Các nguyên tắc quyền riêng tư của tiêu chuẩn này

6.1 Tổng quan về các nguyên tắc quyền riêng tư

Các nguyên tắc quyền riêng tư được mô tả trong tiêu chuẩn này được xây dựng dựa trên các nguyên tắc hiện có do một số quốc gia và tổ chức quốc tế phát triển. Khuôn khổ này tập trung vào việc triển khai các nguyên tắc quyền riêng tư trong hệ thống ICT và phát triển hệ thống quản lý quyền riêng tư để thực hiện trong các hệ thống ICT của tổ chức.
Các nguyên tắc quyền riêng tư này nên được sử dụng làm hướng dẫn cho việc thiết kế, phát triển và triển khai chính sách quyền riêng tư cũng như các biện pháp kiểm soát quyền riêng tư. Ngoài ra, chúng cũng có thể được dùng làm cơ sở để theo dõi và đánh giá hiệu quả, so sánh chuẩn mực và kiểm toán các chương trình quản lý quyền riêng tư trong tổ chức.

Mặc dù có sự khác biệt về yếu tố xã hội, văn hóa, kinh tế và các yếu tố khác có thể hạn chế việc áp dụng các nguyên tắc này trong một số bối cảnh, vẫn khuyến nghị áp dụng tất cả các

nguyên tắc được xác định trong tiêu chuẩn này. Các ngoại lệ đối với các nguyên tắc này nên bị hạn chế ở mức tối thiểu.
Các nguyên tắc quyền riêng tư được liệt kê trong Bảng 3 dưới đây làm cơ sở cho tiêu chuẩn này.

Bảng 3 — Các nguyên tắc quyền riêng tư của ISO/IEC 29100

1. Chấp thuận và lựa chọn
2. Tính hợp pháp và xác định mục đích
3. Hạn chế thu thập
4. Giảm thiểu dữ liệu
5. Hạn chế sử dụng, lưu giữ và tiết lộ
6. Tính chính xác và chất lượng
7. Cởi mở, minh bạch và thông báo
8. Tham gia và truy cập cá nhân
9. Trách nhiệm giải trình
10. An ninh thông tin
11. Tuân thủ quyền riêng tư

6.2 Chấp thuận và lựa chọn

Việc tuân thủ nguyên tắc chấp thuận bao gồm:

— Cung cấp cho chủ thể PII quyền lựa chọn việc cho phép hay không cho phép xử lý PII của họ, trừ khi chủ thể PII không thể tự do từ chối chấp thuận hoặc luật áp dụng cho phép xử lý PII mà không cần sự chấp thuận của thể nhân đó. Quyết định của chủ thể PII phải được đưa ra tự do, cụ thể và dựa trên hiểu biết đầy đủ.

— Lấy sự chấp thuận tham gia của chủ thể PII cho việc thu thập hoặc xử lý các thông tin PII nhạy cảm, trừ khi luật áp dụng cho phép xử lý PII nhạy cảm mà không cần sự chấp thuận của thể nhân.

— Thông báo cho chủ thể PII về quyền của họ theo nguyên tắc tham gia và quyền truy cập cá nhân trước khi họ quyết định đồng ý hay không.

— Cung cấp cho chủ thể PII các thông tin được chỉ ra trong nguyên tắc minh bạch, rõ ràng và thông báo trước khi họ quyết định đồng ý hay không.

— Giải thích cho chủ thể PII các tác động khi họ quyết định đồng ý hoặc từ chối.

Cần có các biện pháp để chủ thể PII được phép lựa chọn cách thức xử lý PII của họ và cho phép họ rút lại sự chấp thuận một cách dễ dàng và miễn phí. Yêu cầu này phải được xử lý theo chính sách quyền riêng tư.

Ngay cả khi sự chấp thuận bị rút lại, bên kiểm soát PII vẫn có thể cần lưu giữ một số PII trong một khoảng thời gian để tuân thủ các nghĩa vụ pháp lý hoặc hợp đồng (ví dụ: lưu trữ dữ liệu,

trách nhiệm giải trình). Trong trường hợp xử lý PII không dựa trên sự chấp thuận mà dựa trên cơ sở pháp lý khác, chủ thể PII nên được thông báo khi có thể.

Khi chủ thể PII rút lại sự chấp thuận, PII phải được loại trừ khỏi việc xử lý cho bất kỳ mục đích nào mà sự chấp thuận ban đầu đã bao phủ.

GHI CHÚ: Các yêu cầu pháp lý về xử lý dữ liệu có thể được áp dụng.

Đối với bên kiểm soát PII, việc tuân thủ nguyên tắc lựa chọn bao gồm:

— Cung cấp cho chủ thể PII các cơ chế rõ ràng, dễ thấy, dễ hiểu, dễ tiếp cận và chi phí hợp lý để họ thực hiện lựa chọn và đưa ra sự chấp thuận liên quan đến việc xử lý PII của mình vào thời điểm thu thập, sử dụng lần đầu hoặc sớm nhất có thể sau đó.

— Thực hiện các sở thích của chủ thể PII như đã được thể hiện trong sự chấp thuận của họ.

Các quy định bổ sung có thể được xác định cho việc xử lý PII không dựa trên sự chấp thuận (ví dụ: thực hiện hợp đồng, bảo vệ quyền lợi thiết yếu của chủ thể PII, hoặc tuân thủ pháp luật). Trong một số trường hợp, luật áp dụng quy định rằng sự chấp thuận của chủ thể PII không đủ cơ sở pháp lý để xử lý PII (ví dụ: sự chấp thuận của trẻ vị thành niên được đưa ra mà không có sự đồng ý của cha mẹ hoặc người giám hộ).

Hơn nữa, cần xem xét các yêu cầu bổ sung liên quan đến việc chuyển giao PII ra quốc tế. Bên kiểm soát PII có trách nhiệm tuân thủ các quy định bổ sung này trước khi xử lý hoặc chuyển giao dữ liệu.

6.3 Tính hợp pháp và xác định mục đích

Việc tuân thủ nguyên tắc tính hợp pháp và xác định mục đích bao gồm:

— Đảm bảo rằng mục đích (hoặc các mục đích) tuân thủ luật áp dụng và dựa trên cơ sở pháp lý được phép

— Thông báo mục đích (hoặc các mục đích) cho chủ thể PII trước thời điểm thông tin được thu thập hoặc sử dụng lần đầu cho một mục đích mới

— Sử dụng ngôn ngữ cho các yêu cầu kỹ thuật này một cách rõ ràng và phù hợp với các tình huống cụ thể; và

— Nếu cần, cung cấp giải thích đầy đủ về lý do phải xử lý PII nhạy cảm. Đối với PII nhạy cảm, có thể áp dụng các quy định nghiêm ngặt hơn đối với mục đích xử lý.

GHI CHÚ: Các yêu cầu pháp lý cụ thể hoặc sự cho phép của cơ quan thẩm quyền có thể được áp dụng.

6.4 Hạn chế thu thập

Việc tuân thủ nguyên tắc hạn chế thu thập bao gồm:

— Hạn chế việc thu thập PII trong phạm vi pháp luật hiện hành và chỉ thu thập những thông tin thực sự cần thiết cho các mục đích đã xác định.

Các tổ chức không nên thu thập PII một cách tùy tiện. Cả số lượng và loại PII được thu thập nên giới hạn trong những gì cần thiết để thực hiện các mục đích (hợp pháp) do bên kiểm

soát PII xác định. Các tổ chức nên xem xét cẩn thận loại PII nào sẽ cần thiết để đạt được một mục đích cụ thể trước khi tiến hành thu thập. Đồng thời, các tổ chức nên ghi chép loại PII thu thập được và lý do thu thập như một phần của chính sách và thực hành quản lý thông tin.

Có thể xảy ra trường hợp bên kiểm soát PII muốn thu thập thêm PII cho các mục đích khác ngoài việc cung cấp dịch vụ cụ thể mà chủ thể PII yêu cầu (ví dụ: cho mục đích tiếp thị trực tiếp). Tùy theo khu vực pháp lý, việc thu thập thông tin bổ sung này có thể chỉ được thực hiện với sự đồng ý của chủ thể PII. Đồng thời, việc thu thập một số thông tin nhất định có thể được yêu cầu theo luật áp dụng. Trong phạm vi có thể, chủ thể PII nên được phép lựa chọn có cung cấp thông tin bổ sung đó hay không, và cần được thông báo rõ ràng rằng việc trả lời yêu cầu cung cấp thông tin bổ sung là tùy chọn.

6.5 Giảm thiểu dữ liệu

Việc tuân thủ nguyên tắc giảm thiểu dữ liệu bao gồm thiết kế và triển khai các quy trình xử lý dữ liệu và hệ thống ICT sao cho:

— Giảm thiểu lượng PII được xử lý và số lượng các bên liên quan về quyền riêng tư cũng như số người được phép tiếp cận hoặc xử lý PII.

— Đảm bảo áp dụng nguyên tắc “chỉ được biết khi cần thiết” (tức là mỗi người chỉ được phép xử lý PII cần thiết cho việc thực hiện nhiệm vụ chính thức của họ trong khuôn khổ mục đích hợp pháp của việc xử lý PII).

— Sử dụng hoặc cung cấp các tùy chọn mặc định, khi có thể, cho các tương tác và giao dịch không liên quan đến việc xác định chủ thể PII, giảm khả năng quan sát hành vi của họ và hạn chế khả năng liên kết các PII được thu thập.

— Tiêu hủy PII một cách an toàn khi có thể thực hiện, đặc biệt là khi mục đích xử lý PII đã kết thúc và không còn yêu cầu pháp lý phải lưu giữ dữ liệu.

Giảm thiểu dữ liệu có mối liên hệ chặt chẽ với nguyên tắc hạn chế thu thập dữ liệu. Trong khi hạn chế thu thập tập trung vào việc giới hạn dữ liệu được thu thập liên quan đến mục đích đã xác định, giảm thiểu dữ liệu tập trung vào việc tối thiểu hóa quá trình xử lý PII.

6.6 Hạn chế sử dụng, lưu giữ và tiết lộ

Việc tuân thủ nguyên tắc hạn chế sử dụng, lưu giữ và tiết lộ bao gồm:

— Hạn chế việc sử dụng, lưu giữ và tiết lộ (bao gồm chuyển giao) PII chỉ trong phạm vi cần thiết để thực hiện các mục đích cụ thể, rõ ràng và hợp pháp.

— Hạn chế việc sử dụng PII chỉ cho các mục đích do bên kiểm soát PII xác định trước khi thu thập.

GHI CHÚ: Các yêu cầu pháp lý như bắt buộc lưu giữ PII cho các mục đích khác nhau có thể được áp dụng.

— Chỉ lưu giữ PII trong thời gian cần thiết để thực hiện các mục đích đã nêu, sau đó tiêu hủy hoặc ẩn danh PII một cách an toàn.

— Khoá PII (tức là lưu trữ, bảo mật và loại trừ PII khỏi các xử lý tiếp theo) bất cứ khi nào và trong thời gian các mục đích đã nêu kết thúc, nhưng vẫn phải lưu giữ nếu luật áp dụng yêu cầu.

Khi PII được chuyển giao quốc tế, bên kiểm soát PII phải lưu ý các yêu cầu quốc gia hoặc địa phương bổ sung liên quan đến chuyển giao xuyên biên giới.

6.7 Độ chính xác và chất lượng

Việc tuân thủ nguyên tắc độ chính xác và chất lượng bao gồm:

— Đảm bảo rằng PII được xử lý là chính xác, đầy đủ, cập nhật (trừ khi có cơ sở hợp pháp để giữ dữ liệu cũ), phù hợp và liên quan đến mục đích sử dụng.
— Đảm bảo độ tin cậy của PII thu thập từ nguồn khác ngoài chủ thể PII trước khi xử lý.
— Xác minh, bằng các phương tiện thích hợp, tính hợp lệ và chính xác của các thông tin do chủ thể PII cung cấp trước khi thực hiện bất kỳ thay đổi nào đối với PII (để đảm bảo các thay đổi được ủy quyền đúng), khi điều này phù hợp.

— Thiết lập các quy trình thu thập PII để giúp đảm bảo độ chính xác và chất lượng.

— Thiết lập cơ chế kiểm soát để định kỳ kiểm tra độ chính xác và chất lượng của PII đã thu thập và lưu trữ.

Nguyên tắc này đặc biệt quan trọng trong các trường hợp dữ liệu có thể được sử dụng để cấp hoặc từ chối một lợi ích đáng kể cho thể nhân, hoặc dữ liệu không chính xác có thể gây ra thiệt hại đáng kể cho thể nhân.

6.8 Cởi mở, minh bạch và thông báo

Việc tuân thủ nguyên tắc về sựu cởi mở, tính minh bạch và thông báo bao gồm:

— Cung cấp cho chủ thể PII thông tin rõ ràng và dễ tiếp cận về các chính sách, quy trình và thực tiễn của bên kiểm soát PII liên quan đến việc xử lý PII.

— Trong các thông báo, cần nêu rõ rằng PII đang được xử lý, mục đích của việc xử lý, những ai có thể được tiếp cận PII, và thông tin liên hệ của bên kiểm soát PII.

— Thông báo các lựa chọn và công cụ mà bên kiểm soát PII cung cấp để chủ thể PII có thể hạn chế việc xử lý, cũng như truy cập, chỉnh sửa hoặc xoá thông tin của mình.

— Thông báo cho chủ thể PII khi có các thay đổi lớn trong quy trình xử lý PII.

Tính minh bạch, bao gồm thông tin chung về logic cơ bản của việc xử lý PII, có thể được yêu cầu, đặc biệt nếu quá trình xử lý đó liên quan đến một quyết định có ảnh hưởng đến chủ thể PII. Các bên liên quan về quyền riêng tư có thực hiện xử lý PII nên công khai sẵn các thông tin cụ thể về chính sách và thực hành liên quan đến việc quản lý PII cho người dùng.

Tất cả các nghĩa vụ hợp đồng liên quan đến việc xử lý PII cần được ghi chép đầy đủ và thông báo nội bộ một cách phù hợp. Những nghĩa vụ này cũng nên được thông báo ra bên ngoài, trong phạm vi các thông tin này không phải là thông tin mật.

Ngoài ra, mục đích của việc xử lý PII cần được trình bày chi tiết đủ để chủ thể PII hiểu được:

— Các PII cụ thể cần thiết cho mục đích đã xác định;

— Mục đích cụ thể của việc thu thập PII;

— Quy trình xử lý cụ thể (bao gồm các cơ chế thu thập, truyền đạt và lưu trữ);

— Các loại thể nhân được ủy quyền sẽ truy cập PII và những thể nhân mà PII có thể được chuyển giao; và

— Các yêu cầu cụ thể về lưu giữ và tiêu hủy PII.

6.9 Sự tham gia và quyền truy cập của cá nhân

Việc tuân thủ nguyên tắc tham gia và truy cập của cá nhân bao gồm:

— Cho phép chủ thể PII truy cập và xem lại PII của mình, với điều kiện xác thực danh tính trước bằng mức độ đảm bảo thích hợp và quyền truy cập không bị cấm theo luật hiện hành;

— Cho phép chủ thể PII phản đối về tính chính xác và đầy đủ của PII và yêu cầu sửa đổi, hiệu chỉnh hoặc xoá dữ liệu nếu phù hợp và khả thi trong bối cảnh cụ thể;

— Cung cấp bất kỳ sửa đổi, hiệu chỉnh hoặc xoá PII nào cho các bên xử lý PII và bên thứ ba mà PII đã được tiết lộ, nếu các bên này được biết đến; và

— Thiết lập các quy trình để chủ thể PII thực hiện các quyền này một cách đơn giản, nhanh chóng và hiệu quả, không gây chậm trễ hoặc tốn kém không cần thiết.

Bên kiểm soát PII cần áp dụng các biện pháp kiểm soát phù hợp để đảm bảo chủ thể PII chỉ truy cập PII của chính mình, không phải của người khác, trừ khi người truy cập được ủy quyền thay mặt cho một chủ thể PII không thể tự thực hiện quyền truy cập.

Luật pháp hiện hành có thể trao quyền cho chủ thể PII truy cập, xem xét và phản đối việc xử lý PII trong một số trường hợp nhất định. Khi một phản đối không được giải quyết thỏa đáng theo ý chủ thể PII, nội dung phản đối chưa được giải quyết cần được ghi lại bởi tổ chức. Khi thích hợp, sự tồn tại của phản đối chưa được giải quyết này nên được truyền đến các bên xử lý PII và bên thứ ba khác có quyền truy cập vào thông tin liên quan.

6.10 Trách nhiệm giải trình

Việc xử lý PII đòi hỏi trách nhiệm thận trọng và việc áp dụng các biện pháp cụ thể, thực tế để bảo vệ dữ liệu.

Việc tuân thủ nguyên tắc trách nhiệm giải trình bao gồm:

— Lập hồ sơ và truyền đạt, khi cần thiết, tất cả các chính sách, quy trình và thực tiễn liên quan đến quyền riêng tư;

— Giao nhiệm vụ thực hiện các chính sách, thủ tục và thực tiễn liên quan đến quyền riêng tư cho một thể nhân cụ thể trong tổ chức (người này có thể ủy quyền cho người khác trong tổ chức nếu phù hợp);

— Khi chuyển giao PII cho bên thứ ba, đảm bảo bên nhận sẽ tuân thủ mức độ bảo vệ quyền riêng tư tương đương thông qua hợp đồng hoặc các biện pháp khác, chẳng hạn như các

chính sách nội bộ bắt buộc (luật pháp hiện hành có thể có các yêu cầu bổ sung liên quan đến việc chuyển giao dữ liệu quốc tế);

— Tổ chức đào tạo phù hợp cho nhân viên của đơn vị kiểm soát PII, những người sẽ có quyền truy cập vào PII;

— Thiết lập các quy trình xử lý khiếu nại và bồi thường nội bộ hiệu quả dành cho các chủ thể dữ liệu cá nhân;

— Thông báo cho các chủ thể dữ liệu cá nhân về các vi phạm quyền riêng tư có thể gây ra thiệt hại đáng kể cho họ (trừ khi bị cấm, ví dụ như khi hợp tác với cơ quan thực thi pháp luật) cũng như các biện pháp đã được thực hiện để giải quyết.

— Thông báo cho tất cả các bên liên quan về quyền riêng tư về các vi phạm quyền riêng tư theo yêu cầu tại một số khu vực pháp lý (ví dụ: các cơ quan bảo vệ dữ liệu) và tùy thuộc vào mức độ rủi ro;

— Cho phép chủ thể PII bị thiệt hại được tiếp cận các biện pháp trừng phạt và/hoặc khắc phục thích hợp và hiệu quả, chẳng hạn như chỉnh sửa, xóa bỏ hoặc bồi thường nếu vi phạm quyền riêng tư đã xảy ra; và.

— Xem xét các quy trình bồi thường trong những trường hợp không thể hoàn nguyên quyền riêng tư của thể nhân về trạng thái ban đầu như chưa từng có vi phạm xảy ra.

Các biện pháp khắc phục vi phạm quyền riêng tư cần được thực hiện phù hợp với mức độ rủi ro liên quan, nhưng phải triển khai càng nhanh càng tốt (trừ khi bị cấm, ví dụ như cản trở một cuộc điều tra hợp pháp).

Việc thiết lập các quy trình khắc phục là một phần quan trọng trong việc đảm bảo trách nhiệm giải trình. Khắc phục cung cấp cho chủ thể PII cách thức để yêu cầu bên kiểm soát PII chịu trách nhiệm khi có hành vi sử dụng sai PII. Bồi thường là một hình thức khắc phục, bao gồm cung cấp đền bù cho chủ thể PII bị ảnh hưởng. Điều này quan trọng không chỉ trong trường hợp trộm cắp danh tính, tổn hại uy tín hoặc sử dụng sai PII, mà còn khi xảy ra sai sót trong việc chỉnh sửa hoặc thay đổi PII tương ứng.

Khi có các quy trình khắc phục, chủ thể PII có thể cảm thấy yên tâm hơn khi thực hiện giao dịch, vì rủi ro được cảm nhận đối với họ đã được giảm đáng kể. Với một số dịch vụ, việc khắc phục dễ thực hiện hơn (ví dụ: tổn thất tài chính) so với các trường hợp khác (ví dụ: bị đánh cắp danh tính, ảnh hưởng đến hình ảnh hoặc uy tín của thể nhân), trong đó khả năng định lượng và bồi thường cho tổn thất có thể khó khăn hơn một chút. Việc khắc sẽ phục hiệu quả nhất khi dựa trên minh bạch và trung thực.

Lưu ý: Các loại biện pháp khắc phục cần thiết có thể được quy định bởi pháp luật.

6.11 An toàn thông tin

Việc tuân thủ nguyên tắc an toàn thông tin bao gồm:

— Bảo vệ PII thuộc quyền quản lý của tổ chức bằng các biện pháp kiểm soát phù hợp ở cấp độ vận hành, chức năng và chiến lược nhằm đảm bảo tính toàn vẹn, bảo mật và khả năng sẵn có của PII, đồng thời bảo vệ PII khỏi các rủi ro như truy cập trái phép, phá hủy, sử dụng, thay đổi, tiết lộ hoặc mất mát trong toàn bộ vòng đời của PII;

— Lựa chọn các bên xử lý PII đảm bảo đủ các biện pháp kiểm soát về tổ chức, vật lý và kỹ thuật cho việc xử lý PII, đồng thời đảm bảo tuân thủ các biện pháp kiểm soát này;

— Dựa trên các biện pháp kiểm soát dựa trên các tiêu chuẩn an ninh, kết quả đánh giá rủi ro an ninh hệ thống theo ISO 31000 và kết quả phân tích chi phí/lợi ích;

Lưu ý: Các yêu cầu pháp lý có thể được áp dụng.

— Thực hiện các biện pháp bảo vệ PII tùy theo mức rủi ro có thể xảy ra và mức độ nghiêm trọng nếu rủi ro xảy ra, dựa trên tính nhạy cảm của dữ liệu, số lượng chủ thể PII có thể bị ảnh hưởng và bối cảnh mà PII được lưu giữ;

— Hạn chế quyền truy cập PII đối với những cá nhân cần quyền truy cập đó để thực hiện nhiệm vụ của mình, và hạn chế quyền truy cập của những cá nhân đó chỉ đối với PII mà họ cần truy cập để thực hiện nhiệm vụ của mình;

— Khắc phục các rủi ro và lỗ hổng được phát hiện thông qua các đánh giá rủi ro về quyền riêng tư và quy trình kiểm toán; và

— Đưa các biện pháp kiểm soát vào đánh giá và rà soát định kỳ trong quá trình quản lý rủi ro an toàn liên tục.

6.12 Tuân thủ quyền riêng tư

Việc tuân thủ nguyên tắc bảo vệ quyền riêng tư bao gồm:

— Xác minh và chứng minh rằng việc xử lý PII đáp ứng các yêu cầu về bảo vệ dữ liệu và đảm bảo quyền riêng tư thông qua các kiểm toán định kỳ, sử dụng kiểm toán viên nội bộ hoặc bên thứ ba đáng tin cậy;

— Thiết lập các biện pháp kiểm soát nội bộ và cơ chế giám sát độc lập phù hợp để đảm bảo tuân thủ pháp luật về quyền riêng tư cũng như các chính sách và quy trình về bảo mật, bảo vệ dữ liệu và quyền riêng tư; và

— Xây dựng và duy trì các đánh giá rủi ro quyền riêng tư nhằm đánh giá xem các chương trình và dịch vụ liên quan đến xử lý PII có tuân thủ các yêu cầu về bảo vệ dữ liệu và quyền riêng tư hay không.

Luật pháp hiện hành có thể quy định rằng một hoặc nhiều cơ quan giám sát chịu trách nhiệm theo dõi việc việc tuân thủ luật bảo vệ dữ liệu. Trong những trường hợp này, đáp ứng nguyên tắc tuân thủ quyền riêng tư còn có nghĩa là hợp tác với các cơ quan giám sát đó và tuân thủ hướng dẫn cũng như yêu cầu của họ.

PHỤ LỤC A
(Tham khảo)

Sự tương ứng giữa các khái niệm của ISO/IEC 29100 và các khái niệm của ISO/IEC 27000

Để thuận tiện hơn khi sử dụng ISO/IEC 27000 và các tiêu chuẩn quốc tế liên quan trong bối cảnh quyền riêng tư, Bảng A.1 trình bày mối quan hệ giữa các khái niệm chính của chúng.

Bảng A.1 — Tương ứng các khái niệm của ISO/IEC 29100 với các khái niệm của ISO/IEC 27000

ISO/IEC 29100 Khái niệm	**Tương ứng với các khái niệm ISO/IEC 27000**
Các bên liên quan đến quyền riêng tư	Các bên liên quan
PII (Thông tin nhận dạng cá nhân)	Tài sản thông tin
Vi phạm quyền riêng tư	Sự cố an toàn thông tin
Kiểm soát quyền riêng tư	Kiểm soát
Rủi ro quyền riêng tư	Rủi ro
Đánh giá tác động quyền riêng tư	Quản lý rủi ro
Yêu cầu bảo vệ quyền riêng tư	Mục tiêu kiểm soát

Tài liệu tham khảo

[1] ISO Guide 73, Risk management — Vocabulary

[2] ISO 31000, Risk management — Guidelines

[3] SC 27 committee document 502 — Privacy References List, available at: https://committee.iso.org/ home/jtc1sc27

[4] ISO/IEC 27000:2018, Information technology — Security techniques — Information security management systems — Overview and vocabulary

[5] ISO/IEC 27001, Information security, cybersecurity and privacy protection — Information security management systems — Requirements

[6] ISO/IEC 27002, Information security, cybersecurity and privacy protection — Information security controls

[7] ISO/IEC 27003, Information technology — Security techniques — Information security management systems — Guidance

[8] ISO/IEC 27004, Information technology — Security techniques — Information security management
Monitoring, measurement, analysis and evaluation

[9] ISO/IEC 27005, Information security, cybersecurity and privacy protection — Guidance on managing information security risks

[10] ISO/IEC 27006, Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems

[11] ISO/IEC 27007, Information security, cybersecurity and privacy protection — Guidelines for information security management systems auditing

[12] ISO/IEC TS 27008, Information technology — Security techniques — Guidelines for the assessment of information security controls

[13] ISO/IEC 27009[4)], Information technology — Security techniques — Sector-specific application of ISO/IEC 27001 — Requirements

[14] ISO/IEC 27010, Information technology — Security techniques — Information security management for inter-sector and inter-organizational communications

[15] ISO/IEC 27011, Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for telecommunications organizations

[16] ISO/IEC 27013, Information security, cybersecurity and privacy protection — Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1

[17] ISO/IEC 27014, Information security, cybersecurity and privacy protection — Governance of information security

[18] ISO/IEC TR 27016, Information technology — Security techniques — Information security management — Organizational economics

[19] ISO/IEC 27017, Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services

[20] ISO/IEC 27018, Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors

[21] ISO/IEC 27019, Information technology — Security techniques — Information security controls for the energy utility industry

[22] ISO/IEC 27021, Information technology — Security techniques — Competence requirements for information security management systems professionals

[23] ISO/IEC 27701, Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines

[24] ISO 27799, Health informatics — Information security management in health using ISO/IEC 27002

[25] ISO/IEC 29151, Information technology — Security techniques — Code of practice for personally identifiable information protection