Áp dụng Hệ thống quản lý thông tin riêng tư ISO/IEC 27701:2019 trong hỗ trợ tuân thủ Nghị định 13/2023/ND-CP

Trình bày: Mr. Đoàn Văn Khải,
Business Development Director
Head of ICT

By Royal Charter

bsi.

Chương trình

1. Giới thiệu chương trình
2. Nghị định 13/2023/NĐ-CP và tầm quan trọng của việc tuân thủ
3. Giới thiệu về Tiêu chuẩn ISO/IEC 27701:2019 và vai trò của Hệ thống quản lý thông tin riêng tư (PIMS)
4. Lợi ích của áp dụng Tiêu chuẩn ISO/IEC 27701:2019 trong việc đáp ứng yêu cầu của nghị định 13/2023/NĐ-CP
5. Câu hỏi và trả lời

1. Giới thiệu chương trình

Mr. Đạt

2. Nghị định 13/2023/NĐ-CP và tầm quan trọng của việc tuân thủ

- Ban hành ngày 17/04/2023
- Hiệu lực từ ngày 01/07/2023
- Nội dung cơ bản: 04 chương, bao gồm 44 điều
- Chương 1: Những Qui định chung (8 điều)
- Chương 2: Hoạt động bảo vệ dữ liệu cá nhân (04 mục, 23 điều)
- Chương 3: Trách nhiệm của cơ quan, tổ chức, cá nhân (11 điều):
- Chương 4: Điều khoản thi Hành (02 điều)

CHÍNH PHỦ

Số: 13/2023/NĐ-CP

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

Hà Nội, ngày 17 tháng 4 năm 2023

NGHỊ ĐỊNH
Bảo vệ dữ liệu cá nhân

Căn cứ Luật Tổ chức Chính phủ ngày 19 tháng 6 năm 2015; Luật sửa đổi, bổ sung một số điều của Luật Tổ chức Chính phủ và Luật Tổ chức chính quyền địa phương ngày 22 tháng 11 năm 2019;

Căn cứ Bộ luật Dân sự ngày 24 tháng 11 năm 2015;

Căn cứ Luật An ninh quốc gia ngày 03 tháng 12 năm 2004;

Căn cứ Luật An ninh mạng ngày 12 tháng 6 năm 2018;

Theo đề nghị của Bộ trưởng Bộ Công an;

Chính phủ ban hành Nghị định bảo vệ dữ liệu cá nhân.

bsi.

Một số điểm nổi bật của Nghị định 13/2023/NĐ-CP

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

1. Nghị định này quy định về bảo vệ dữ liệu cá nhân và trách nhiệm bảo vệ dữ liệu cá nhân của cơ quan, tổ chức, cá nhân có liên quan.

2. Nghị định này áp dụng đối với:

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

b) Cơ quan, tổ chức, cá nhân nước ngoài tại Việt Nam;

c) Cơ quan, tổ chức, cá nhân Việt Nam hoạt động tại nước ngoài;

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

Một số điểm nổi bật của Nghị định 13/2023/NĐ-CP

Điều 2. Giải thích từ ngữ

1. Dữ liệu cá nhân là thông tin dưới dạng ký hiệu, chữ viết, chữ số, hình ảnh, âm thanh hoặc dạng tương tự trên môi trường điện tử gắn liền với một con người cụ thể hoặc giúp xác định một con người cụ thể. Dữ liệu cá nhân bao gồm dữ liệu cá nhân cơ bản và dữ liệu cá nhân nhạy cảm.

2. Thông tin giúp xác định một con người cụ thể là thông tin hình thành từ hoạt động của cá nhân mà khi kết hợp với các dữ liệu, thông tin lưu trữ khác có thể xác định một con người cụ thể.

Một số điểm nổi bật của Nghị định 13/2023/NĐ-CP

Xác định loại dữ liệu cá nhân được xử lý

Tương ứng với các định nghĩa trong GDPR, Nghị định 13 phân biệt rõ ràng các vai trò khác nhau của những các bên tham gia vào xử lý dữ liệu và quy định trách nhiệm riêng cho từng vai trò.

Bao gồm:

- Bên Kiểm soát dữ liệu
- Bên Xử lý dữ liệu
- Bên Kiểm soát và xử lý dữ liệu
- Bên thứ ba

Một số điểm nổi bật của Nghị định 13/2023/NĐ-CP

Xác định vai trò trong quá trình xử lý dữ liệu cá nhân

Dữ liệu cá nhân là các thông tin liên quan đến một con người cụ thể hoặc giúp xác định một con người cụ thể khi các thông tin này được sử dụng độc lập hoặc kết hợp với các thông tin khác có thể là thông tin trực tiếp, chữ số, chữ viết, hình ảnh, âm thanh, video và dữ liệu kỹ thuật số.

Nghị định 13 phân loại dữ liệu cá nhân thành hai (2) loại: (1) dữ liệu cá nhân cơ bản và (2) dữ liệu cá nhân nhạy cảm; đồng thời liệt kê các dữ liệu chính yếu thuộc hai loại này.

Dữ liệu cá nhân cơ bản bao gồm: thông tin định danh thông thường

Dữ liệu cá nhân nhạy cảm được định nghĩa là dữ liệu cá nhân gắn liền với quyền riêng tư của cá nhân mà khi bị xâm phạm sẽ gây ảnh hưởng trực tiếp tới quyền và lợi ích hợp pháp của cá nhân

Nghị định 13 áp dụng các nghĩa vụ xử lý và bảo vệ bổ sung đối với việc xử lý dữ liệu cá nhân nhạy cảm.

Một số điểm nổi bật của Nghị định 13/2023/NĐ-CP

Xác định căn cứ pháp lý cho việc xử lý dữ liệu cá nhân

Nghị định 13 yêu cầu các tổ chức phải có sự đồng ý trước từ phía cá nhân để xử lý dữ liệu của cá nhân đó, và phải tuân thủ các nguyên tắc được nêu trong Điều 3, tức là: quá trình xử lý dữ liệu phải

(i) đúng quy định pháp luật;

(ii) minh bạch;

(iii) chỉ được thực hiện cho (các) mục đích đã tuyên bố;

(iv) giới hạn trong mục đích và phạm vi nhất định;

(v) sử dụng dữ liệu được cập nhật, bổ sung phù hợp với mục đích; và

(vi) phải bảo mật; đồng thời

(vii) đảm bảo dữ liệu chỉ được lưu trữ trong khoảng thời gian phù hợp và

(viii) các tổ chức chịu trách nhiệm giải trình về tính tuân thủ này.

Một số điểm nổi bật của Nghị định 13/2023/NĐ-CP

Xác định cơ chế để cá nhân có thể rút lại sự đồng ý

Khi có yêu cầu rút lại sự đồng ý phát sinh, tổ chức cần phải thông báo cho cá nhân về hậu quả hoặc thiệt hại có thể xảy đến từ việc rút lại sự đồng ý.

Khi sự đồng ý được sử dụng làm cơ sở pháp lý để xử lý dữ liệu cá nhân, cần có cơ chế để các cá nhân rút lại sự đồng ý của họ và cho phép việc rút lại có thể được in hoặc sao chép khi cần.

Hệ thống phải có khả năng thông báo cho cá nhân về hậu quả hoặc thiệt hại có thể xảy ra khi rút lại sự đồng ý.

Một số điểm nổi bật của Nghị định 13/2023/NĐ-CP

Yêu cầu về thông báo xử lý dữ liệu cá nhân

Nghị định 13 yêu cầu các tổ chức cung cấp thông báo tuân thủ cho các cá nhân trước khi xử lý dữ liệu cá nhân của họ.

Thông báo về xử lý dữ liệu sẽ bao gồm loại, mục đích và phương pháp xử lý; danh tính của Bên xử lý dữ liệu cá nhân hoặc bên thứ ba có liên quan; rủi ro trong quá trình xử lý, thời gian xử lý.

Một số điểm nổi bật của Nghị định 13/2023/NĐ-CP

Xử lý yêu cầu của chủ thể dữ liệu

Nghị định 13 đưa ra một số quyền của chủ thể dữ liệu (ví dụ như: quyền truy cập, quyền hạn chế xử lý dữ liệu, quyền phản đối xử lý dữ liệu, quyền chỉnh sửa dữ liệu, quyền xóa dữ liệu, v.v.) và yêu cầu bên xử lý dữ liệu phải đảm bảo các quyền này.

Mọi yêu cầu hạn chế hoặc phản đối xử lý dữ liệu được thực hiện trong 72 giờ sau khi có yêu cầu của chủ thể dữ liệu

Một số điểm nổi bật của Nghị định 13/2023/NĐ-CP

Nhân sự phụ trách bảo vệ dữ liệu cá nhân

Bổ nhiệm nhân sự phụ trách bảo vệ dữ liệu cá nhân hoặc chỉ định bộ phận có chức năng tương tự.

Thời gian ân hạn 2 năm chỉ áp dụng cho trường hợp thành lập doanh nghiệp siêu nhỏ, doanh nghiệp nhỏ, doanh nghiệp vừa, công ty khởi nghiệp không trực tiếp tham gia cung cấp dịch vụ xử lý dữ liệu cá nhân.

Các tổ chức đều được yêu cầu bổ nhiệm nhân sự phụ trách bảo vệ dữ liệu cá nhân.

Một số điểm nổi bật của Nghị định 13/2023/NĐ-CP

Bảo vệ dữ liệu và báo cáo vi phạm quy định về bảo vệ dữ liệu

Nghị định 13 yêu cầu ***Bên Kiểm soát dữ liệu cá nhân*** và ***Bên Kiểm soát và xử lý dữ liệu cá nhân*** phải đảm bảo an toàn dữ liệu cá nhân và thông báo cho cơ quan chức năng về bất kỳ vi phạm quy định về bảo vệ dữ liệu cá nhân trong vòng 72 giờ sau khi xảy ra hành vi vi phạm.

Bên Xử lý dữ liệu cá nhân phải thông báo cho Bên Kiểm soát dữ liệu cá nhân một cách nhanh nhất có thể sau khi nhận thấy có sự vi phạm quy định về bảo vệ dữ liệu cá nhân để họ có thể đáp ứng yêu cầu 72 giờ này.

Trường hợp thông báo chậm thì Bên Kiểm soát dữ liệu cá nhân phải đưa ra lý do.

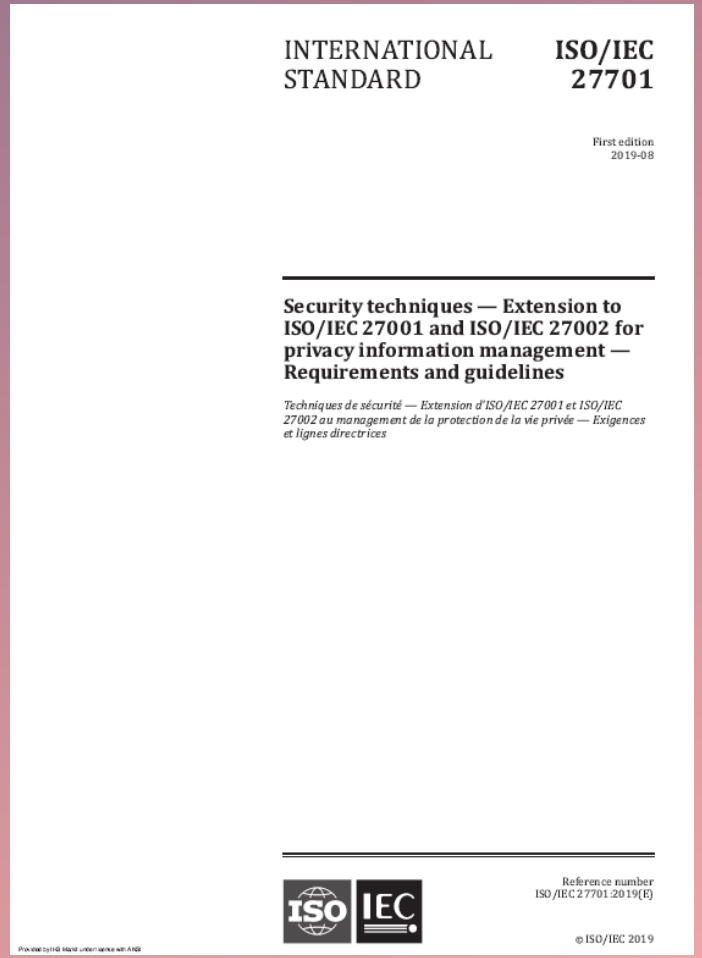
Một số điểm nổi bật của Nghị định 13/2023/NĐ-CP

Báo cáo đánh giá tác động cho cơ quan chức năng về xử lý dữ liệu cá nhân và chuyển dữ liệu cá nhân ra ngước ngoài

Bên Kiểm soát dữ liệu và Bên Xử lý dữ liệu đều phải tiến hành đánh giá tác động bảo vệ dữ liệu cá nhân đối với tất cả các hoạt động xử lý của mình, bao gồm tự xử lý dữ liệu cá nhân cơ bản và nhạy cảm hoặc bằng cách ký hợp đồng với bên xử lý dữ liệu cá nhân hoặc cung cấp thông tin cho bên thứ ba hoặc chuyển dữ liệu cá nhân ra nước ngoài và gửi trong vòng 60 ngày kể từ khi bắt đầu hoạt động xử lý dữ liệu.

3. Giới thiệu về Tiêu chuẩn ISO/IEC 27701:2019 và vai trò của Hệ thống quản lý thông tin riêng tư (PIMS)

- ISO/IEC 27701 là tiêu chuẩn quốc tế cho Hệ thống quản lý thông tin riêng tư (PIMS)
- Đây là một phần mở rộng về sự riêng tư đối với ISO/IEC 27001 Quản lý An toàn thông tin và ISO/IEC 27002 Các biện pháp kiểm soát.
- Tiêu chuẩn này cung cấp hướng dẫn và các yêu cầu về bảo vệ riêng tư, bao gồm cách các tổ chức nên quản lý thông tin cá nhân và hỗ trợ chứng minh việc tuân thủ các quy định về sự riêng tư trên khắp thế giới.


INTERNATIONAL STANDARD

ISO/IEC 27701

First edition
2019-08

Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines

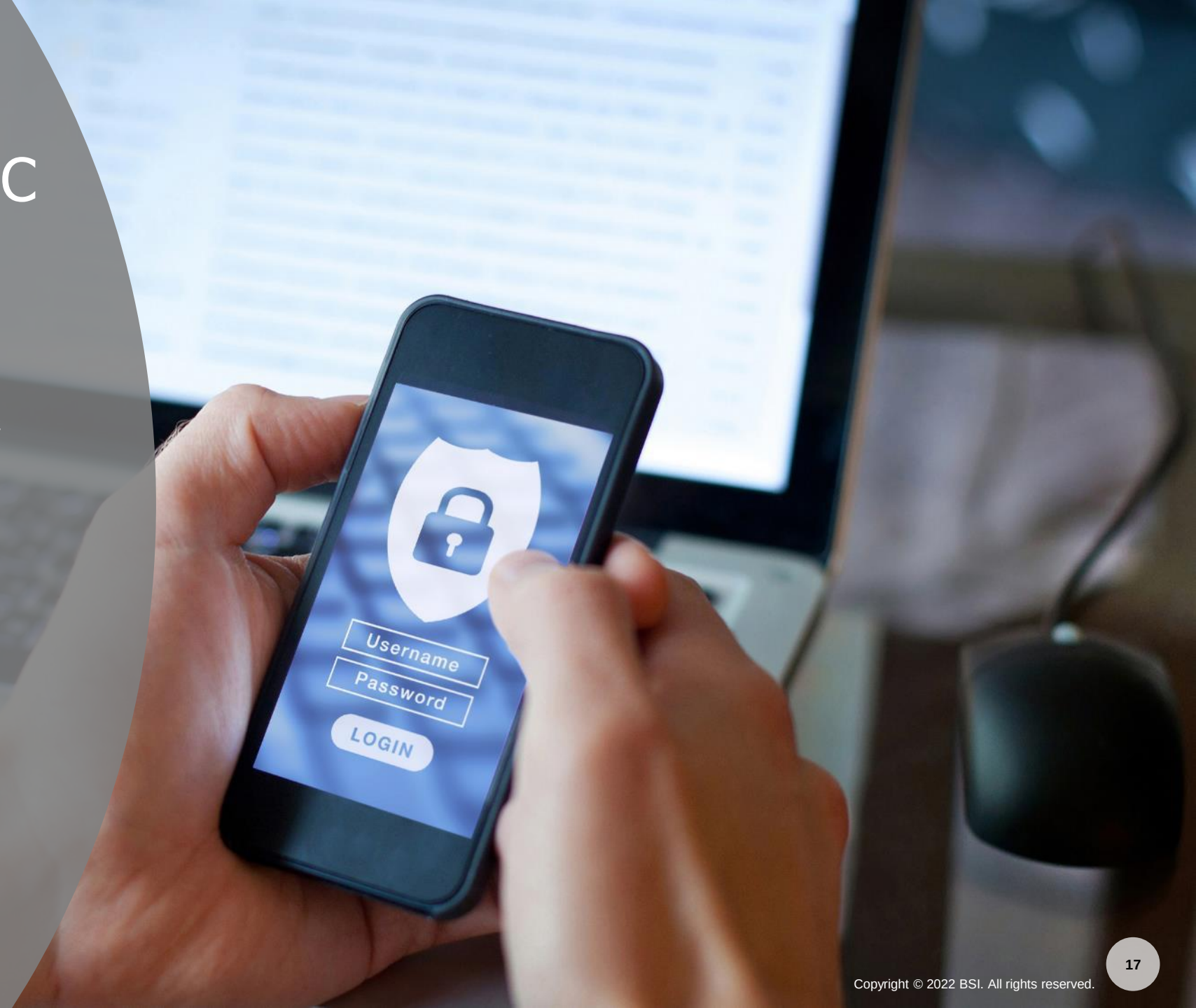
Techniques de sécurité — Extension d'ISO/IEC 27001 et ISO/IEC 27002 au management de la protection de la vie privée — Exigences et lignes directrices

Reference number
ISO/IEC 27701:2019(E)

© ISO/IEC 2019

Mục đích của ISO/IEC 27701

- Cung cấp hướng dẫn thực hành tốt nhất
- Xây dựng lòng tin
- Các thỏa thuận kinh doanh hiệu quả hơn
- Tạo bằng chứng
- Cách hiệu quả để quản lý các quá trình liên quan đến thông tin cá nhân PII



bsi.

Lợi ích của việc áp dụng ISO/IEC 27701

Thông tin cá nhân?

1. Dữ liệu cá nhân là thông tin dưới dạng ký hiệu, chữ viết, chữ số, hình ảnh, âm thanh hoặc dạng tương tự trên môi trường điện tử gắn liền với một con người cụ thể hoặc giúp xác định một con người cụ thể. Dữ liệu cá nhân bao gồm dữ liệu cá nhân cơ bản và dữ liệu cá nhân nhạy cảm.

2. Thông tin giúp xác định một con người cụ thể là thông tin hình thành từ hoạt động của cá nhân mà khi kết hợp với các dữ liệu, thông tin lưu trữ khác có thể xác định một con người cụ thể.

Nghị định số 13/2023/NĐ-CP

Bất kỳ thông tin nào (a) có thể được sử dụng để xác định chủ thể PII mà thông tin đó có liên quan, hoặc (b) là hoặc có thể được liên kết trực tiếp hoặc gián tiếp với chủ thể PII

ISO29100:2011

2.9
personally identifiable information
PII
any information that (a) can be used to identify the PII principal to whom such information relates, or (b) is or might be directly or indirectly linked to a PII principal

Vì sao phải bảo vệ thông tin cá nhân?

- Các tổ chức/ doanh nghiệp thương mại luôn muốn nắm bắt, thu thập, sử dụng, phân tích, khai thác TTCN của khách hàng hiện tại và các khách hàng tiềm năng
- Mỗi cá nhân rất không muốn các TTCN của mình bị rơi vào tay người lạ
- Yêu cầu pháp lý

Yêu cầu pháp lý

>132

Luật và quy định về sự riêng tư trên toàn cầu

Lên tới 4% doanh thu hoặc 20 triệu €

Tiền phạt/ chế tài

- **Tuân thủ:** Luật về sự riêng tư Quốc tế như GDPR, California Consumer Privacy Act, Australian Privacy Act, Japanese Privacy Law (APPI)
- **Rủi ro về về danh tiếng: Mất uy tín thương hiệu hoặc có thể bị phạt** (tới 4% doanh thu hoặc €20 triệu)

Làm thế nào để bảo vệ và thể hiện trách nhiệm và xây dựng lòng tin trong quản lý thông tin cá nhân ?

→ ISO/IEC 27701

Ai sẽ sử dụng ISO/IEC 27701?

- Các tổ chức, bất kể loại hình và qui mô.
- Các công ty nhà nước và tư nhân, các tổ chức chính phủ và các tổ chức phi lợi nhuận.
- Các tổ chức chịu trách nhiệm xử lý Thông tin cá nhân (PII) trong hệ thống quản lý an toàn thông tin (ISMS), cụ thể:
  - Các Bên kiểm soát PII (bao gồm các Bên đồng kiểm soát PII)
  - Các Bên xử lý PII

Khuôn khổ về sự riêng tư


INTERNATIONAL STANDARD

ISO/IEC 29100

First edition
2011-12-15

Information technology — Security techniques — Privacy framework

Technologies de l'information — Techniques de sécurité — Cadre privé

ISO/IEC 29100:

- Xác định một thuật ngữ về sự riêng tư phổ biến
- Xác định các tác nhân và vai trò của họ trong việc xử lý thông tin nhận dạng cá nhân (PII)
- Mô tả các cân nhắc về bảo vệ riêng tư
- Cung cấp các tham chiếu đến các nguyên tắc an toàn đã biết đối với công nghệ thông tin

Điều 3. Nguyên tắc bảo vệ dữ liệu cá nhân

1. Dữ liệu cá nhân được xử lý theo quy định của pháp luật.

2. Chủ thể dữ liệu được biết về hoạt động liên quan tới xử lý dữ liệu cá nhân của mình, trừ trường hợp luật có quy định khác.

3. Dữ liệu cá nhân chỉ được xử lý đúng với mục đích đã được Bên Kiểm soát dữ liệu cá nhân, Bên Xử lý dữ liệu cá nhân, Bên Kiểm soát và xử lý dữ liệu cá nhân, Bên thứ ba đăng ký, tuyên bố về xử lý dữ liệu cá nhân.

4. Dữ liệu cá nhân thu thập phải phù hợp và giới hạn trong phạm vi, mục đích cần xử lý. Dữ liệu cá nhân không được mua, bán dưới mọi hình thức, trừ trường hợp luật có quy định khác.

5. Dữ liệu cá nhân được cập nhật, bổ sung phù hợp với mục đích xử lý.

6. Dữ liệu cá nhân được áp dụng các biện pháp bảo vệ, bảo mật trong quá trình xử lý, bao gồm cả việc bảo vệ trước các hành vi vi phạm quy định về bảo vệ dữ liệu cá nhân và phòng, chống sự mất mát, phá hủy hoặc thiệt hại do sự cố, sử dụng các biện pháp kỹ thuật.

7. Dữ liệu cá nhân chỉ được lưu trữ trong khoảng thời gian phù hợp với mục đích xử lý dữ liệu, trừ trường hợp pháp luật có quy định khác.

8. Bên Kiểm soát dữ liệu, Bên Kiểm soát và xử lý dữ liệu cá nhân phải chịu trách nhiệm tuân thủ các nguyên tắc xử lý dữ liệu được quy định từ khoản 1 tới khoản 7 Điều này và chứng minh sự tuân thủ của mình với các nguyên tắc xử lý dữ liệu đó.

ISO/IEC 29100
(Các nguyên tắc về sự riêng tư)

1. Sự đồng ý và lựa chọn
2. Tính hợp pháp của mục đích và đặc điểm
3. Giới hạn việc thu thập
4. Giảm thiểu dữ liệu
5. Giới hạn sử dụng, lưu giữ và tiết lộ
6. Độ chính xác và chất lượng
7. Công khai, minh bạch và thông báo
8. Sự tham gia và quyền truy cập của cá nhân
9. Trách nhiệm giải trình
10. An toàn thông tin
11. Tuân thủ riêng tư

bsi.

Các thuật ngữ chính và thuật ngữ thay thế

Thuật ngữ được ISO 27701 sử dụng	Thuật ngữ thay thế
Privacy information management system (PIMS) Hệ thống quản lý thông tin riêng tư	Personal information management system (PIMS) Hệ thống quản lý thông tin cá nhân
Personally identifiable information (PII) Thông tin có thể định danh cá nhân/ Thông tin cá nhân	Personal data Dữ liệu cá nhân
PII principal Chủ sở hữu/ Chủ thể PII	**Data subject** Đối tượng dữ liệu
Privacy by design riêng tư theo thiết kế	Data protection by design Bảo vệ dữ liệu theo thiết kế
Privacy by default riêng tư theo mặc định	Data protection by default Bảo vệ dữ liệu theo mặc định
PII controller Bên kiểm soát PII	**Data controller** Bên kiểm soát dữ liệu
PII processor Bên xử lý PII	**Data processor** Bên xử lý dữ liệu

đối chiếu các nguyên tắc về sự riêng tư theo ISO/IEC 27701

1. Sự đồng ý và lựa chọn
2. Tính hợp pháp của mục đích và đặc điểm
3. Giới hạn việc thu thập
4. Giảm thiểu dữ liệu
5. Giới hạn sử dụng, lưu giữ và tiết lộ
6. Độ chính xác và chất lượng
7. Công khai, minh bạch và thông báo
8. Sự tham gia và quyền truy cập của cá nhân
9. Trách nhiệm giải trình
10. An toàn thông tin
11. Tuân thủ riêng tư

ISO/IEC 27701:2019

Phụ lục C
(thông tin)
đối chiếu các nguyên tắc cho
Bên kiểm soát PII – **Bảng C**
Bên xử lý PII – **Bảng D**

Phụ lục D
(thông tin)
đối chiếu các điều khoản tới GDPR

ISO/IEC 27701

Xác định các yêu cầu và cung cấp hướng dẫn cho thiết lập, áp dụng, duy trì và cải tiến liên tục một hệ thống quản lý thông tin về sự riêng tư (PIMS)

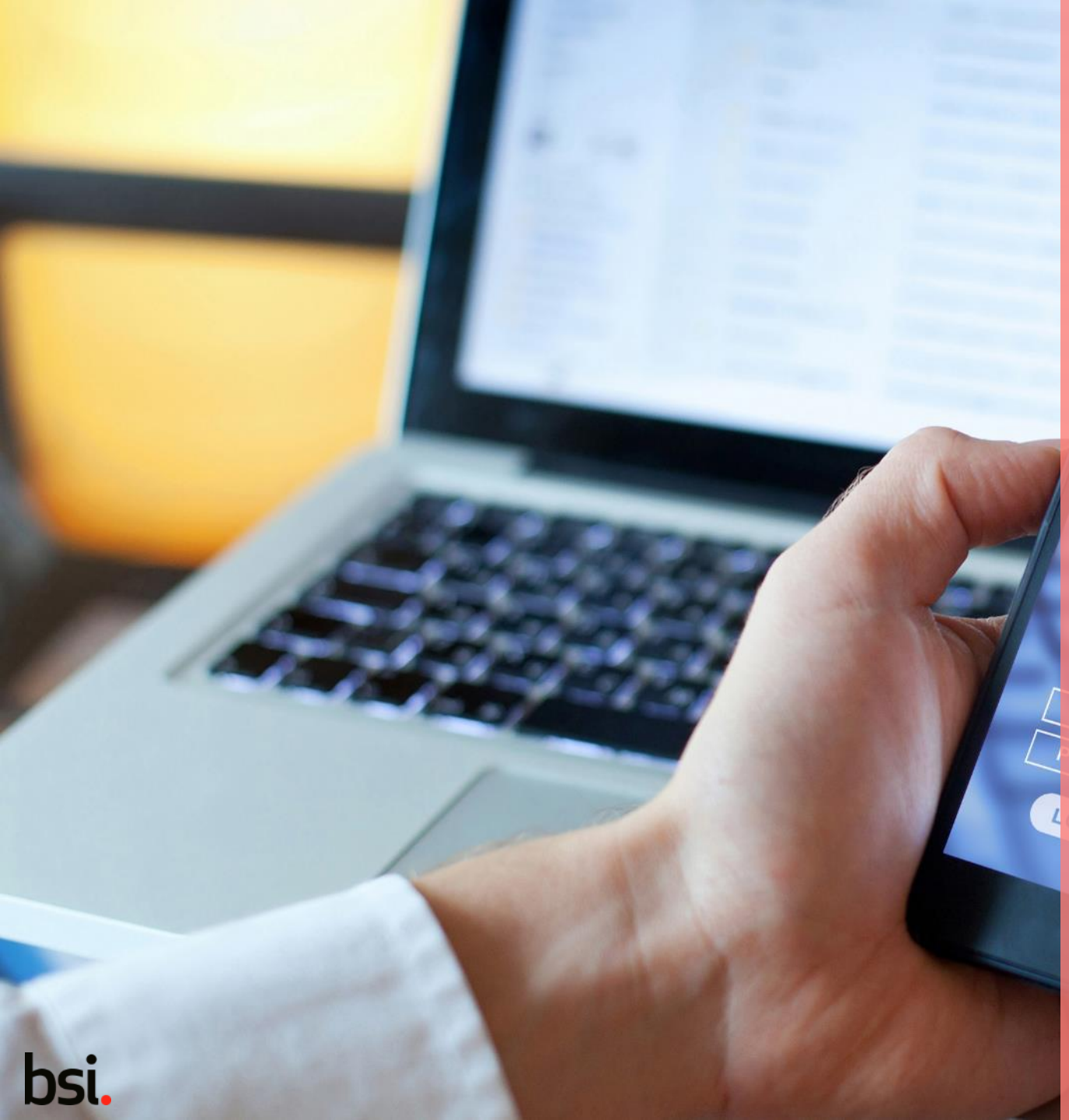
PIMS giải quyết vấn đề bảo vệ riêng tư có thể bị ảnh hưởng bởi quá trình xử lý PII

Phần mở rộng của ISO / IEC 27001 và không thể được sử dụng riêng lẻ

Xử lý (Processing)

- Hoạt động hoặc tập hợp các hoạt động được thực hiện dựa trên thông tin nhận dạng cá nhân (PII).
- Ví dụ về hoạt động xử lý PII bao gồm, nhưng không giới hạn:
  - Thu thập
  - Lưu trữ
  - Thay đổi
  - Truy xuất
  - Tham vấn
  - Tiết lộ
  - Ẩn danh
  - Bút danh
  - Phổ biến hoặc cung cấp thông tin
  - Xóa hoặc phá hủy
  - Bằng mọi cách tự động hoặc thủ công

ISO/IEC 29100



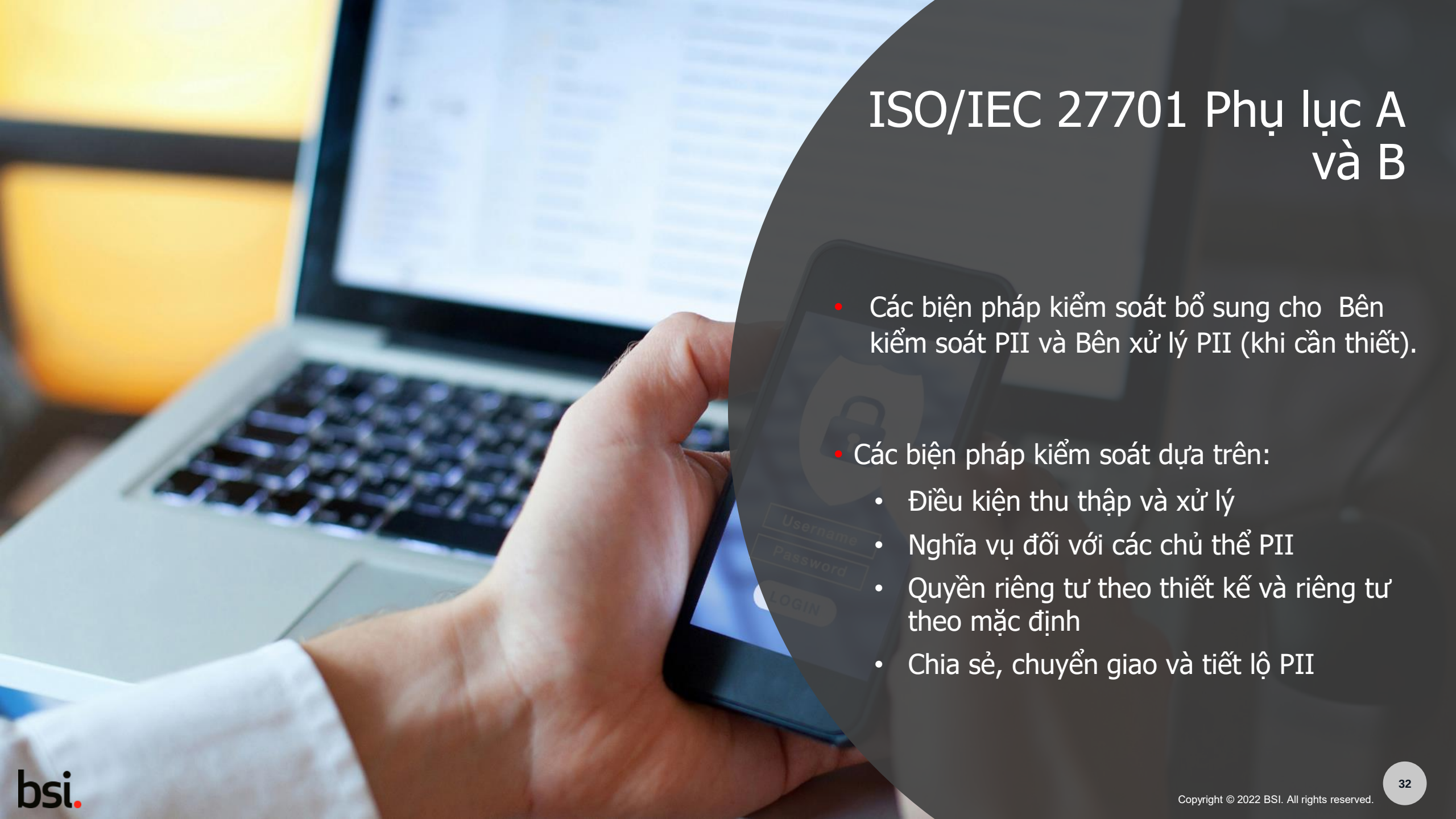
Áp dụng ISO/IEC 27701 cho ISO/IEC 27001

- Phần mở rộng chung: An toàn thông tin bao gồm sự riêng tư
- Các điều khoản của Hệ thống quản lý thông tin riêng tư (PIMS)
- Toàn bộ 114 biện pháp kiểm soát ISO / IEC 27001 Phụ lục A, ISO / IEC 27002 trong đó có 32 hướng dẫn bổ sung
- Phụ lục ISO / IEC 27701 - Bổ sung, các biện pháp kiểm soát cho Bên kiểm soát và Bên xử lý PII
- Phụ lục A có 31 biện pháp kiểm soát - Phụ lục B có 18 biện pháp kiểm soát
  - Điều kiện thu thập và xử lý

Cấu trúc

Các điều khoản và biện pháp kiểm soát

- Dựa trên các yêu cầu an toàn thông tin trong ISO/IEC 27001
  - Điều khoản 5: PIMS-các yêu cầu cụ thể đối với Bên kiểm soát và Bên xử lý PII
- Dự trên các biện pháp kiểm soát an toàn thông tin trong ISO/IEC 27002
  - Điều khoản 6: PIMS-Các hướng dẫn cụ thể đối với Bên kiểm soát và Bên xử lý PII
  - Điều khoản 7: Hướng dẫn cho Bên kiểm soát PII
  - Điều khoản 8: Hướng dẫn cho Bên xử lý PII
- PIMS các biện pháp cụ thể và các mục tiêu kiểm soát (Qui phạm)
  - Phụ lục A: Bên kiểm soát PII
  - Phụ lục B: Bên xử lý PII



ISO/IEC 27701 Phụ lục A và B

- Các biện pháp kiểm soát bổ sung cho Bên kiểm soát PII và Bên xử lý PII (khi cần thiết).

- Các biện pháp kiểm soát dựa trên:
  - Điều kiện thu thập và xử lý
  - Nghĩa vụ đối với các chủ thể PII
  - Quyền riêng tư theo thiết kế và riêng tư theo mặc định
  - Chia sẻ, chuyển giao và tiết lộ PII

đối chiếu tới các tiêu chuẩn và thuật ngữ khác

Phụ lục C – F (thông tin)

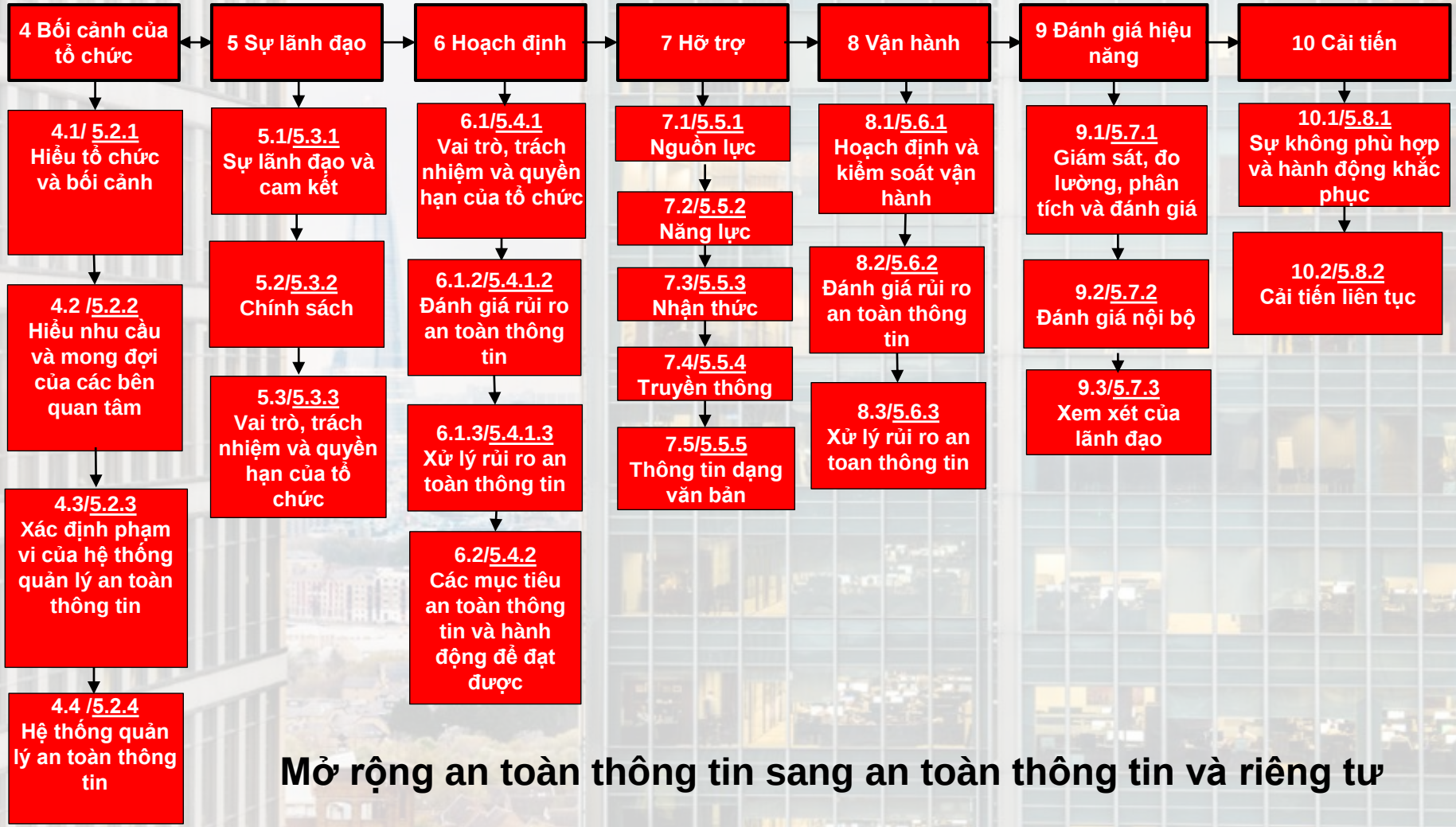
Phụ lục C – đối chiếu ISO/IEC 29100

Phụ lục D – Phụ lục D: đối chiếu tới GDPR

Phụ lục E – đối chiếu ISO/IEC 27018 và ISO/IEC 29151

Phụ lục F – làm thế nào để áp dụng ISO/IEC 27701 cho ISO/IEC 27001 và ISO/IEC 27002

Cách tiếp cận ISMS và cấu trúc bổ sung trong PIMS



Mở rộng an toàn thông tin sang an toàn thông tin và riêng tư

4. Lợi ích của áp dụng Tiêu chuẩn ISO/IEC 27701:2019 trong việc đáp ứng yêu cầu của nghị định 13/2023/NĐ-CP

- Khuôn khổ bảo mật thông tin theo tiêu chuẩn Quốc tế được thừa nhận toàn cầu

3. Hài hòa với thông lệ, quy định quốc tế về bảo vệ dữ liệu cá nhân

Bảo vệ dữ liệu cá nhân là vấn đề được các tổ chức và nhiều quốc gia trên thế giới quan tâm và đi trước nước ta trong thời gian khá dài, có nhiều kinh nghiệm pháp lý và thực tiễn triển khai thi hành để tiếp thu. Do hệ thống pháp luật, trình độ nhận thức, kinh tế, xã hội khác nhau nên việc tiếp thu cần bảo đảm yếu tố hài hòa, trên cơ sở phù hợp với thực tiễn của nước ta. Hầu hết các công ước, khuyến nghị và tiêu chuẩn khu vực về quyền riêng tư và bảo vệ thông tin và dữ liệu cá nhân đều tuân thủ Nguyên tắc bảo mật của Tổ chức hợp tác và phát triển kinh tế (OECD), bao gồm Công ước của Hội đồng châu Âu về bảo vệ cá nhân liên quan đến tự động xử lý thông tin và dữ liệu cá nhân (sau đây là Công ước 108), Hướng dẫn của Liên hợp quốc về các tệp thông tin và dữ liệu cá nhân được vi tính hóa, Khung bảo mật hợp tác kinh tế châu Á-Thái Bình Dương (APEC), Các tiêu chuẩn quốc tế về quyền riêng tư và bảo vệ thông tin và dữ liệu cá nhân (Nghị quyết Madrid), Luật của Tổ chức các quốc gia Hoa Kỳ (OAS) về bảo vệ thông tin và dữ liệu cá nhân năm 2014, và gần đây là Quy định bảo vệ dữ liệu chung của EU (GDPR). Hiện nay, đã có hơn **80** quốc gia ban hành văn bản quy phạm pháp luật về bảo vệ dữ liệu cá nhân, nhiều văn bản có quy định áp dụng đối với tổ chức, cá nhân Việt Nam. Điều này đặt ra yêu cầu đối với Nghị định bảo vệ dữ liệu cá nhân, bảo đảm hài hòa với thông lệ quốc tế nhưng cũng phải tạo môi trường kinh doanh bình đẳng, thượng tôn pháp luật tại Việt Nam.

ND 13/2023/ND-CP vs ISO/IEC 27701:2019

Điều 3. Nguyên tắc bảo vệ dữ liệu cá nhân	ISO/IEC 27001
1. Dữ liệu cá nhân được xử lý theo quy định của pháp luật.	**Áp dụng** - Hệ thống quản lý an toàn thông tin ISO/IEC 27001:2013 (ISO 27001:2022) - Hệ thống quản lý thông tin riêng tư ISO/IEC 27701:2019 - Bổ sung các yêu cầu đặc thù của luật
2. Chủ thể dữ liệu được biết về hoạt động liên quan tới xử lý dữ liệu cá nhân của mình, trừ trường hợp luật có quy định khác.	**A.7.3.3: Cung cấp thông tin cho chủ thể PII** Tổ chức phải cung cấp cho các chủ thể PII thông tin rõ ràng và dễ truy cập để xác định bên kiểm soát PII và mô tả quá trình xử lý PII của họ.
3. Dữ liệu cá nhân chỉ được xử lý đúng với mục đích đã được Bên Kiểm soát dữ liệu cá nhân, Bên Xử lý dữ liệu cá nhân, Bên Kiểm soát và xử lý dữ liệu cá nhân, Bên thứ ba đăng ký, tuyên bố về xử lý dữ liệu cá nhân.	**A.7.4.2: Giới hạn việc xử lý** Tổ chức phải giới hạn việc xử lý PII ở mức đầy đủ, phù hợp và cần thiết cho các mục đích đã xác định.
4. Dữ liệu cá nhân thu thập phải phù hợp và giới hạn trong phạm vi, mục đích cần xử lý. Dữ liệu cá nhân không được mua, bán dưới mọi hình thức, trừ trường hợp luật có quy định khác.	**A.7.4.1: Giới hạn việc thu thập** Tổ chức phải giới hạn việc thu thập PII đến mức tối thiểu có liên quan, tỷ lệ thuận và cần thiết cho các mục đích đã xác định.

Điều 3. Nguyên tắc bảo vệ dữ liệu cá nhân	ISO/IEC 27001
5. Dữ liệu cá nhân được cập nhật, bổ sung phù hợp với mục đích xử lý.	**A.7.4.3: Độ chính xác và chất lượng** Tổ chức phải đảm bảo và lập hồ sơ rằng PII là chính xác, đầy đủ và cập nhật cần thiết cho các mục đích mà nó được xử lý, trong suốt vòng đời của PII.
6. Dữ liệu cá nhân được áp dụng các biện pháp bảo vệ, bảo mật trong quá trình xử lý, bao gồm cả việc bảo vệ trước các hành vi vi phạm quy định về bảo vệ dữ liệu cá nhân và phòng, chống sự mất mát, phá hủy hoặc thiệt hại do sự cố, sử dụng các biện pháp kỹ thuật.	**Áp dụng** - Hệ thống quản lý an toàn thông tin ISO/IEC 27001:2013 (ISO 27001:2022) - Hệ thống quản lý thông tin riêng tư ISO/IEC 27701:2019
7. Dữ liệu cá nhân chỉ được lưu trữ trong khoảng thời gian phù hợp với mục đích xử lý dữ liệu, trừ trường hợp pháp luật có quy định khác.	**A.7.4.7: Lưu giữ** Tổ chức không được lưu giữ PII lâu hơn mức cần thiết cho các mục đích mà PII được xử lý **A.7.4.8: Loại bỏ** Tổ chức phải có các chính sách, quy trình và / hoặc cơ chế được lập thành văn bản để loại bỏ PII.

Điều 3. Nguyên tắc bảo vệ dữ liệu cá nhân	ISO/IEC 27001
8. Bên Kiểm soát dữ liệu, Bên Kiểm soát và xử lý dữ liệu cá nhân phải chịu trách nhiệm tuân thủ các nguyên tắc xử lý dữ liệu được quy định từ khoản 1 tới khoản 7 Điều này và chứng minh sự tuân thủ của mình với các nguyên tắc xử lý dữ liệu đó	Phụ lục A Các mục tiêu kiểm soát và biện pháp kiểm soát tham chiếu cụ thể của PIMS (bên kiểm soát PII) Phụ lục B Các mục tiêu kiểm soát và biện pháp kiểm soát tham chiếu cụ thể của PIMS (bên xử lý PII)

Điều 9. Quyền của chủ thể dữ liệu	ISO/IEC 27001
1. Quyền được biết 2. Quyền đồng ý 3. Quyền truy cập 4. Quyền rút lại sự đồng ý 5. Quyền xóa dữ liệu 6. Quyền hạn chế xử lý dữ liệu 7. Quyền cung cấp dữ liệu 8. Quyền phản đối xử lý dữ liệu 9. Quyền khiếu nại, tố cáo, khởi kiện 10. Quyền yêu cầu bồi thường thiệt hại 11. Quyền tự bảo vệ	A.7.3.1 Xác định và thực hiện các nghĩa vụ đối với chủ thể PII A.7.3.2 Xác định thông tin cho các chủ thể PII A.7.3.3 Cung cấp bản sao của PII đã được xử lý A.7.3.4 Cung cấp cơ chế để sửa đổi hoặc rút lại sự đồng ý A.7.3.5 Cung cấp cơ chế phản đối việc xử lý PII A.7.3.6 Truy cập, sửa chữa và/hoặc xóa A.7.3.7 Nghĩa vụ của bên kiểm soát PII trong việc thông báo cho bên thứ ba A.7.3.8 Cung cấp bản sao của PII đã được xử lý A.7.3.9 Giải quyết các yêu cầu

Điều 11. Sự đồng ý của chủ thể dữ liệu	ISO/IEC 27701
1. Sự đồng ý của chủ thể dữ liệu được áp dụng đối với tất cả các hoạt động trong quy trình xử lý dữ liệu cá nhân, trừ trường hợp luật có quy định khác.	**7.2.3 Xác định thời điểm và cách thức đạt được sự đồng ý** Tổ chức phải xác định và ghi lại một quá trình mà qua đó tổ chức có thể chứng minh nếu, khi nào và bằng cách nào sự đồng ý cho việc xử lý PII đã nhận được từ các chủ thể.
2. Sự đồng ý của chủ thể dữ liệu chỉ có hiệu lực khi chủ thể dữ liệu tự nguyện và biết rõ các nội dung sau: a) Loại dữ liệu cá nhân được xử lý; b) Mục đích xử lý dữ liệu cá nhân; c) Tổ chức, cá nhân được xử lý dữ liệu cá nhân; d) Các quyền, nghĩa vụ của chủ thể dữ liệu.	**7.2.4 Có được và ghi lại sự đồng ý** Tổ chức phải có được và ghi lại sự đồng ý từ các chủ thể PII theo các quá trình được lập thành văn bản. **8.2.1 Sự đồng ý của khách hàng** Tổ chức phải đảm bảo, nếu có liên quan, hợp đồng xử lý PII đề cập đến vai trò của tổ chức trong việc hỗ trợ các nghĩa vụ của khách hàng (có tính đến bản chất của quá trình xử lý và thông tin có sẵn cho tổ chức).

Điều 12. Rút lại sự đồng ý	ISO/IEC 27701
1. Việc rút lại sự đồng ý không ảnh hưởng đến tính hợp pháp của việc xử lý dữ liệu đã được đồng ý trước khi rút lại sự đồng ý. 2. Việc rút lại sự đồng ý phải được thể hiện ở một định dạng có thể được in, sao chép bằng văn bản, bao gồm cả dưới dạng điện tử hoặc định dạng kiểm chứng được. 3. Khi nhận yêu cầu rút lại sự đồng ý của chủ thể dữ liệu, Bên Kiểm soát dữ liệu cá nhân, Bên Kiểm soát và xử lý dữ liệu cá nhân thông báo cho chủ thể dữ liệu về hậu quả, thiệt hại có thể xảy ra khi rút lại sự đồng ý. 4. Sau khi thực hiện quy định tại khoản 2 Điều này, Bên Kiểm soát dữ liệu, Bên Xử lý dữ liệu, Bên Kiểm soát và xử lý dữ liệu, Bên thứ ba phải ngừng và yêu cầu các tổ chức, cá nhân có liên quan ngừng xử lý dữ liệu của chủ thể dữ liệu đã rút lại sự đồng ý.	**7.3.4 Cung cấp cơ chế để sửa đổi hoặc rút lại sự đồng ý** Tổ chức phải cung cấp một cơ chế để các chủ thể PII sửa đổi hoặc rút lại sự đồng ý của họ.

Điều 13. Thông báo xử lý dữ liệu cá nhân	ISO/IEC 27701
1. Việc thông báo được thực hiện một lần trước khi tiến hành đối với hoạt động xử lý dữ liệu cá nhân. 2. Nội dung thông báo cho chủ thể dữ liệu về xử lý dữ liệu cá nhân: a) Mục đích xử lý; b) Loại dữ liệu cá nhân được sử dụng có liên quan tới mục đích xử lý quy định tại điểm a khoản 2 Điều này; c) Cách thức xử lý; d) Thông tin về các tổ chức, cá nhân khác có liên quan tới mục đích xử lý quy định tại điểm a khoản 2 Điều này; đ) Hậu quả, thiệt hại không mong muốn có khả năng xảy ra; e) Thời gian bắt đầu, thời gian kết thúc xử lý dữ liệu. 3. Việc thông báo cho chủ thể dữ liệu phải được thể hiện ở một định dạng có thể được in, sao chép bằng văn bản, bao gồm cả dưới dạng điện tử hoặc định dạng kiểm chứng được.	**7.3.3 Cung cấp thông tin cho chủ thể PII** Tổ chức phải cung cấp cho các chủ thể thông tin rõ ràng và dễ tiếp cận nhằm xác định bên kiểm soát PII và mô tả quá trình xử lý PII của họ.

Điều 13. Thông báo xử lý dữ liệu cá nhân	ISO/IEC 27701
4. Bên Kiểm soát dữ liệu cá nhân, Bên Kiểm soát và xử lý dữ liệu cá nhân không cần thực hiện quy định lại khoản 1 Điều này trong các trường hợp sau: a) Chủ thể dữ liệu đã biết rõ và đồng ý toàn bộ với nội dung quy định tại khoản 1 và khoản 2 Điều này trước khi đồng ý cho Bên Kiểm soát dữ liệu cá nhân, Bên Kiểm soát và xử lý dữ liệu cá nhân tiến hành thu thập dữ liệu cá nhân, phù hợp với các quy định tại Điều 9 Nghị định này; b) Dữ liệu cá nhân được xử lý bởi cơ quan nhà nước có thẩm quyền với mục đích phục vụ hoạt động của cơ quan nhà nước theo quy định của pháp luật.	Tiêu chuẩn ISO/IEC 27701 không yêu cầu cụ thể, áp dụng theo qui định của Luật

Điều 14. Cung cấp dữ liệu cá nhân	ISO/IEC 27701
1. Chủ thể dữ liệu được yêu cầu Bên Kiểm soát dữ liệu cá nhân, Bên Kiểm soát và xử lý dữ liệu cá nhân cung cấp cho bản thân dữ liệu cá nhân của mình.	**7.3.3 Cung cấp thông tin cho chủ thể PII** Tổ chức phải cung cấp cho các chủ thể thông tin rõ ràng và dễ tiếp cận nhằm xác định bên kiểm soát PII và mô tả quá trình xử lý PII của họ.
2. Bên Kiểm soát dữ liệu cá nhân, Bên Kiểm soát và xử lý dữ liệu cá nhân: a) Được cung cấp dữ liệu cá nhân của chủ thể dữ liệu cho tổ chức, cá nhân khác khi có sự đồng ý của chủ thể dữ liệu, trừ trường hợp pháp luật có quy định khác; b) Thay mặt chủ thể dữ liệu cung cấp dữ liệu cá nhân của chủ thể dữ liệu cho tổ chức hoặc cá nhân khác khi chủ thể dữ liệu đồng ý cho phép đại diện và ủy quyền, trừ trường hợp pháp luật có quy định khác.	Tiêu chuẩn ISO/IEC 27701 không yêu cầu cụ thể, áp dụng theo qui định của Luật
3. Việc cung cấp dữ liệu cá nhân của chủ thể dữ liệu được Bên Kiểm soát dữ liệu cá nhân, Bên Kiểm soát và xử lý dữ liệu cá nhân thực hiện trong 72 giờ sau khi có yêu cầu của chủ thể dữ liệu, trừ trường hợp luật có quy định khác.	Tiêu chuẩn ISO/IEC 27701 không yêu cầu cụ thể, áp dụng theo qui định của Luật

Điều 14. Cung cấp dữ liệu cá nhân	ISO/IEC 27701
4. Bên Kiểm soát dữ liệu cá nhân, Bên Kiểm soát và xử lý dữ liệu cá nhân không cung cấp dữ liệu cá nhân trong trường hợp: a) Gây tổn hại tới quốc phòng, an ninh quốc gia, trật tự an toàn xã hội; b) Việc cung cấp dữ liệu cá nhân của chủ thể dữ liệu có thể ảnh hưởng tới sự an toàn, sức khỏe thể chất hoặc tinh thần của người khác; c) Chủ thể dữ liệu không đồng ý cung cấp, cho phép đại diện hoặc ủy quyền nhận dữ liệu cá nhân.	Tiêu chuẩn ISO/IEC 27701 không yêu cầu cụ thể, áp dụng theo qui định của Luật
5. Hình thức yêu cầu cung cấp dữ liệu cá nhân: a) Chủ thể dữ liệu trực tiếp hoặc ủy quyền cho người khác đến trụ sở Bên Kiểm soát dữ liệu cá nhân, Bên Kiểm soát và xử lý dữ liệu cá nhân yêu cầu cung cấp dữ liệu cá nhân. Người tiếp nhận yêu cầu có trách nhiệm hướng dẫn tổ chức, cá nhân yêu cầu điền các nội dung vào Phiếu yêu cầu cung cấp dữ liệu cá nhân. Trường hợp tổ chức, cá nhân yêu cầu cung cấp thông tin không biết chữ hoặc bị khuyết tật không thể viết yêu cầu thì người tiếp nhận yêu cầu cung cấp thông tin có trách nhiệm giúp điền các nội dung vào Phiếu yêu cầu cung cấp dữ liệu cá nhân; b) Gửi Phiếu yêu cầu cung cấp dữ liệu cá nhân theo Mẫu số 01, 02 tại Phụ lục của Nghị định này qua mạng điện tử, dịch vụ bưu chính, fax đến Bên Kiểm soát dữ liệu cá nhân, Bên Kiểm soát và xử lý dữ liệu cá nhân.	Tiêu chuẩn ISO/IEC 27701 không yêu cầu cụ thể, áp dụng theo qui định của Luật

Điều 14. Cung cấp dữ liệu cá nhân	ISO/IEC 27701
6. Phiếu yêu cầu cung cấp dữ liệu cá nhân phải được thể hiện bằng tiếng Việt gồm các nội dung chính sau đây: a) Họ, tên; nơi cư trú, địa chỉ; số chứng minh nhân dân, thể căn cước công dân hoặc số hộ chiếu của người yêu cầu; số fax, điện thoại, địa chỉ thư điện tử (nếu có); b) Dữ liệu cá nhân được yêu cầu cung cấp, trong đó chỉ rõ tên văn bản, hồ sơ, tài liệu; c) Hình thức cung cấp dữ liệu cá nhân; d) Lý do, mục đích yêu cầu cung cấp dữ liệu cá nhân	Tiêu chuẩn ISO/IEC 27701 không yêu cầu cụ thể, áp dụng theo qui định của Luật
7. Trường hợp yêu cầu cung cấp dữ liệu cá nhân quy định tại khoản 2 Điều này thì phải kèm theo văn bản đồng ý của cá nhân, tổ chức liên quan.	Tiêu chuẩn ISO/IEC 27701 không yêu cầu cụ thể, áp dụng theo qui định của Luật

Điều 14. Cung cấp dữ liệu cá nhân	ISO/IEC 27701
8. Tiếp nhận yêu cầu cung cấp dữ liệu cá nhân a) Bên Kiểm soát dữ liệu cá nhân, Bên Kiểm soát và xử lý dữ liệu cá nhân có trách nhiệm tiếp nhận yêu cầu cung cấp dữ liệu cá nhân và theo dõi quá trình, danh sách cung cấp dữ liệu cá nhân theo yêu cầu; b) Trường hợp dữ liệu cá nhân được yêu cầu không thuộc thẩm quyền thì Bên Kiểm soát dữ liệu cá nhân, Bên Kiểm soát và xử lý dữ liệu cá nhân nhận được yêu cầu phải thông báo và hướng dẫn tổ chức, cá nhân yêu cầu đến cơ quan có thẩm quyền hoặc thông báo rõ ràng việc không thể cung cấp dữ liệu cá nhân.	Tiêu chuẩn ISO/IEC 27701 không yêu cầu cụ thể, áp dụng theo qui định của Luật
9. Giải quyết yêu cầu cung cấp dữ liệu cá nhân Khi nhận được yêu cầu cung cấp dữ liệu cá nhân hợp lệ, Bên Kiểm soát dữ liệu cá nhân, Bên Kiểm soát và xử lý dữ liệu cá nhân có trách nhiệm cung cấp dữ liệu cá nhân thông báo về thời hạn, địa điểm, hình thức cung cấp dữ liệu cá nhân; chi phí thực tế để in, sao, chụp, gửi thông tin qua dịch vụ bưu chính, fax (nếu có) và phương thức, thời hạn thanh toán; thực hiện việc cung cấp dữ liệu cá nhân theo trình tự, thủ tục quy định tại Điều này.	**7.3.3 Cung cấp thông tin cho chủ thể PII** Tổ chức phải cung cấp cho các chủ thể thông tin rõ ràng và dễ tiếp cận nhằm xác định bên kiểm soát PII và mô tả quá trình xử lý PII của họ. **7.3.9 Giải quyết các yêu cầu** Tổ chức phải xác định và lập thành văn bản các chính sách và quy trình để giải quyết và phản hồi các yêu cầu hợp pháp từ các chủ thể PII.

Điều 16. Lưu trữ, xóa, hủy dữ liệu cá nhân	ISO/IEC 27701
1. Chủ thể dữ liệu được yêu cầu Bên Kiểm soát dữ liệu cá nhân, Bên Kiểm soát và xử lý dữ liệu cá nhân xóa dữ liệu cá nhân của mình trong các trường hợp sau: a) Nhận thấy không còn cần thiết cho mục đích thu thập đã đồng ý và chấp nhận các thiệt hại có thể xảy ra khi yêu cầu xóa dữ liệu; b) Rút lại sự đồng ý; c) Phản đối việc xử lý dữ liệu và Bên Kiểm soát dữ liệu cá nhân, Bên Kiểm soát và xử lý dữ liệu cá nhân không có lý do chính đáng để tiếp tục xử lý; d) Dữ liệu cá nhân được xử lý không đúng với mục đích đã đồng ý hoặc việc xử lý dữ liệu cá nhân là vi phạm quy định của pháp luật; đ) Dữ liệu cá nhân phải xóa theo quy định của pháp luật.	**7.4.8 Huỷ bỏ** Tổ chức phải có các chính sách, quy trình và/hoặc cơ chế được lập thành văn bản để huỷ bỏ PII.

Điều 16. Lưu trữ, xóa, hủy dữ liệu cá nhân	ISO/IEC 27701
2. Việc xóa dữ liệu sẽ không áp dụng khi có đề nghị của chủ thể dữ liệu trong các trường hợp: a) Pháp luật quy định không cho phép xóa dữ liệu; b) Dữ liệu cá nhân được xử lý bởi cơ quan nhà nước có thẩm quyền với mục đích phục vụ hoạt động của cơ quan nhà nước theo quy định của pháp luật; c) Dữ liệu cá nhân đã được công khai theo quy định của pháp luật; d) Dữ liệu cá nhân được xử lý nhằm phục vụ yêu cầu pháp lý, nghiên cứu khoa học, thống kê theo quy định của pháp luật; đ) Trong trường hợp tình trạng khẩn cấp về quốc phòng, an ninh quốc gia, trật tự an toàn xã hội, thảm họa lớn, dịch bệnh nguy hiểm; khi có nguy cơ đe dọa an ninh, quốc phòng nhưng chưa đến mức ban bố tình trạng khẩn cấp; phòng, chống bạo loạn, khủng bố, phòng, chống tội phạm và vi phạm pháp luật; e) Ứng phó với tình huống khẩn cấp đe dọa đến tính mạng, sức khỏe hoặc sự an toàn của chủ thể dữ liệu hoặc cá nhân khác.	Tiêu chuẩn ISO/IEC 27701 không yêu cầu cụ thể, áp dụng theo qui định của Luật

Điều 21. Bảo vệ dữ liệu cá nhân trong kinh doanh dịch vụ tiếp thị, giới thiệu sản phẩm quảng cáo	ISO/IEC 27701
1. Tổ chức, cá nhân kinh doanh dịch vụ tiếp thị, giới thiệu sản phẩm quảng cáo chỉ được sử dụng dữ liệu cá nhân của khách hàng được thu thập qua hoạt động kinh doanh của mình để kinh doanh dịch vụ tiếp thị, giới thiệu sản phẩm quảng cáo khi có sự đồng ý của chủ thể dữ liệu. 2. Việc xử lý dữ liệu cá nhân của khách hàng để kinh doanh dịch vụ tiếp thị, giới thiệu sản phẩm quảng cáo phải được sự đồng ý của khách hàng, trên cơ sở khách hàng biết rõ nội dung, phương thức, hình thức, tần suất giới thiệu sản phẩm. 3. Tổ chức, cá nhân kinh doanh dịch vụ tiếp thị, giới thiệu sản phẩm quảng cáo có trách nhiệm chứng minh việc sử dụng dữ liệu cá nhân của khách hàng được giới thiệu sản phẩm đúng với quy định tại khoản 1 và khoản 2 Điều này.	**A8.2.3 Sử dụng cho tiếp thị và quảng cáo** Tổ chức không được sử dụng PII được xử lý theo hợp đồng cho các mục đích tiếp thị và quảng cáo mà không xác định rằng đã có được sự đồng ý trước của chủ thể PII thích hợp. Tổ chức không được coi việc cung cấp sự đồng ý như vậy là điều kiện để tiếp nhận dịch vụ. Hướng dẫn thực hiện Sự tuân thủ của bên xử lý PII với các yêu cầu hợp đồng của khách hàng cần được ghi lại, đặc biệt là khi tiếp thị và/hoặc quảng cáo được lên kế hoạch. Các tổ chức không nên nhấn mạnh vào việc bao gồm các hoạt động tiếp thị và/hoặc quảng cáo khi chưa có sự đồng ý rõ ràng từ các chủ thể PII.

Điều 23. Thông báo vi phạm quy định về bảo vệ dữ liệu cá nhân	ISO/IEC 27701
1. Trường hợp phát hiện xảy ra vi phạm quy định bảo vệ dữ liệu cá nhân, Bên Kiểm soát dữ liệu cá nhân, Bên Kiểm soát và xử lý dữ liệu cá nhân thông báo cho Bộ Công an (Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao) chậm nhất 72 giờ sau khi xảy ra hành vi vi phạm theo Mẫu số 03 tại Phụ lục của Nghị định này. Trường hợp thông báo sau 72 giờ thì phải kèm theo lý do thông báo chậm, muộn.	**6.13.1.5 Ứng phó sự cố an toàn thông tin** Khi vi phạm PII đã xảy ra, các quy trình ứng phó phải bao gồm các thông báo liên quan và Hồ sơ. Một số khu vực pháp lý xác định các trường hợp khi nào vi phạm phải được thông báo cho cơ quan giám sát và khi nào vi phạm cần được thông báo cho các chủ thể PII. Thông báo phải rõ ràng và có thể được yêu cầu.
2. Bên Xử lý dữ liệu cá nhân phải thông báo cho Bên Kiểm soát dữ liệu cá nhân một cách nhanh nhất có thể sau khi nhận thấy có sự vi phạm quy định về bảo vệ dữ liệu cá nhân.	**6.13.1.5 Ứng phó sự cố an toàn thông tin** Ở một số khu vực pháp lý, bên xử lý PII phải thông báo cho bên kiểm soát PII về sự tồn tại của vi phạm mà không có sự chậm trễ quá mức (tức là càng sớm càng tốt), tốt nhất là ngay khi phát hiện ra để bên kiểm soát PII có thể thực hiện các hành động thích hợp.

Điều 23. Thông báo vi phạm quy định về bảo vệ dữ liệu cá nhân	ISO/IEC 27701
3. Nội dung thông báo vi phạm quy định về bảo vệ dữ liệu cá nhân: a) Mô tả tính chất của việc vi phạm quy định bảo vệ dữ liệu cá nhân, bao gồm: thời gian, địa điểm, hành vi, tổ chức, cá nhân, các loại dữ liệu cá nhân và số lượng dữ liệu liên quan; b) Chi tiết liên lạc của nhân viên được giao nhiệm vụ bảo vệ dữ liệu hoặc tổ chức, cá nhân chịu trách nhiệm bảo vệ dữ liệu cá nhân; c) Mô tả các hậu quả, thiệt hại có thể xảy ra của việc vi phạm quy định bảo vệ dữ liệu cá nhân; d) Mô tả các biện pháp được đưa ra để giải quyết, giảm thiểu tác hại của hành vi vi phạm quy định bảo vệ dữ liệu cá nhân.	**6.13.1.5 Ứng phó sự cố an toàn thông tin** CHÚ THÍCH 2: Thông báo có thể chứa các chi tiết như: một đầu mối liên hệ nơi có thể lấy thêm thông tin; mô tả và hậu quả có thể xảy ra của vi phạm; mô tả về vi phạm bao gồm số lượng cá nhân liên quan cũng như số lượng hồ sơ liên quan; các biện pháp đã thực hiện hoặc dự định thực hiện. CHÚ THÍCH 3: Thông tin về quản lý các sự cố an ninh có thể được tìm thấy trong bộ tiêu chuẩn ISO/IEC 27035.

Điều 23. Thông báo vi phạm quy định về bảo vệ dữ liệu cá nhân	ISO/IEC 27701
4. Trường hợp không thể thông báo đầy đủ các nội dung quy định tại khoản 3 Điều này, việc thông báo có thể được thực hiện theo từng đợt, từng giai đoạn.	Tiêu chuẩn ISO/IEC 27701 không yêu cầu cụ thể, áp dụng theo qui định của Luật
5. Bên Kiểm soát dữ liệu cá nhân, Bên Kiểm soát và xử lý dữ liệu cá nhân phải lập Biên bản xác nhận về việc xảy ra hành vi vi phạm quy định bảo vệ dữ liệu cá nhân, phối hợp với Bộ Công an (Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao) xử lý hành vi vi phạm.	**6.13.1.5 Ứng phó sự cố an toàn thông tin** Trong trường hợp vi phạm liên quan đến PII đã xảy ra, hồ sơ cũng phải bao gồm mô tả về PII bị xâm phạm, nếu biết; và nếu thông báo được thực hiện, các bước được thực hiện để thông báo cho khách hàng và/hoặc các cơ quan quản lý. Ở một số khu vực tài phán, luật pháp và/hoặc quy định hiện hành có thể yêu cầu tổ chức thông báo trực tiếp cho các cơ quan quản lý thích hợp (ví dụ: cơ quan bảo vệ PII) về vi phạm liên quan đến PII.

Điều 23. Thông báo vi phạm quy định về bảo vệ dữ liệu cá nhân	ISO/IEC 27701
6. Tổ chức, cá nhân thông báo cho Bộ Công an (Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao) khi phát hiện các trường hợp sau: a) Phát hiện hành vi vi phạm pháp luật đối với dữ liệu cá nhân; b) Dữ liệu cá nhân bị xử lý sai mục đích, không đúng thỏa thuận ban đầu giữa chủ thể dữ liệu và Bên Kiểm soát dữ liệu cá nhân, Bên Kiểm soát và xử lý dữ liệu cá nhân hoặc vi phạm quy định của pháp luật; c) Không bảo đảm quyền của chủ thể dữ liệu hoặc không được thực hiện đúng; d) Trường hợp khác theo quy định của pháp luật.	Tiêu chuẩn ISO/IEC 27701 không yêu cầu cụ thể, áp dụng theo qui định của Luật

Điều 24. Đánh giá tác động xử lý dữ liệu cá nhân	ISO/IEC 27701
1. Bên Kiểm soát dữ liệu cá nhân, Bên Kiểm soát và xử lý dữ liệu cá nhân lập và lưu giữ Hồ sơ đánh giá tác động xử lý dữ liệu cá nhân của mình kể từ thời điểm bắt đầu xử lý dữ liệu cá nhân. Hồ sơ đánh giá tác động xử lý dữ liệu cá nhân của Bên Kiểm soát dữ liệu cá nhân, Bên Kiểm soát và xử lý dữ liệu cá nhân, bao gồm: a) Thông tin và chi tiết liên lạc của Bên Kiểm soát dữ liệu cá nhân, Bên Kiểm soát và xử lý dữ liệu cá nhân; b) Họ tên, chi tiết liên lạc của tổ chức được phân công thực hiện nhiệm vụ bảo vệ dữ liệu cá nhân và nhân viên bảo vệ dữ liệu cá nhân của Bên Kiểm soát dữ liệu cá nhân, Bên Kiểm soát và xử lý dữ liệu cá nhân; c) Mục đích xử lý dữ liệu cá nhân; d) Các loại dữ liệu cá nhân được xử lý; đ) Tổ chức, cá nhân nhận dữ liệu cá nhân, bao gồm tổ chức, cá nhân ngoài lãnh thổ Việt Nam; e) Trường hợp chuyển dữ liệu cá nhân ra nước ngoài; g) Thời gian xử lý dữ liệu cá nhân; thời gian dự kiến để xoá, hủy dữ liệu cá nhân (nếu có); h) Mô tả về các biện pháp bảo vệ dữ liệu cá nhân được áp dụng; i) Đánh giá mức độ hưởng của việc xử lý dữ liệu cá nhân; hậu quả, thiệt hại không mong muốn có khả năng xảy ra, các biện pháp giảm thiểu hoặc loại bỏ nguy cơ, tác hại đó.	**7.2.5 Đánh giá tác động quyền riêng tư** Tổ chức phải đánh giá sự cần thiết và thực hiện khi thích hợp, đánh giá tác động đến quyền riêng tư bất cứ khi nào việc xử lý PII mới hoặc các thay đổi đối với quá trình xử lý PII hiện tại được lên kế hoạch.

Điều 25. Chuyển dữ liệu cá nhân ra nước ngoài	ISO/IEC 27701
1. Dữ liệu cá nhân của công dân Việt Nam được chuyển ra nước ngoài trong trường hợp Bên chuyển dữ liệu ra nước ngoài lập Hồ sơ đánh giá tác động chuyển dữ liệu cá nhân ra nước ngoài và thực hiện các thủ tục theo quy định tại khoản 3, 4 và 5 Điều này. Bên chuyển dữ liệu ra nước ngoài bao gồm Bên Kiểm soát dữ liệu cá nhân, Bên Kiểm soát và xử lý dữ liệu cá nhân, Bên Xử lý dữ liệu cá nhân, Bên thứ ba.	**7.2.5 Đánh giá tác động quyền riêng tư** Tổ chức phải đánh giá sự cần thiết và thực hiện khi thích hợp, đánh giá tác động đến quyền riêng tư bất cứ khi nào việc xử lý PII mới hoặc các thay đổi đối với quá trình xử lý PII hiện tại được lên kế hoạch. **7.5.1 Xác định cơ sở để chuyển giao PII giữa các khu vực pháp lý** Tổ chức phải xác định và lập thành văn bản cơ sở liên quan cho việc chuyển giao PII giữa các khu vực pháp lý.

Điều 25. Chuyển dữ liệu cá nhân ra nước ngoài	ISO/IEC 27701
2. Hồ sơ đánh giá tác động chuyển dữ liệu cá nhân ra nước ngoài, gồm: a) Thông tin và chi tiết liên lạc của Bên chuyển dữ liệu và Bên tiếp nhận dữ liệu b) Họ tên, chi tiết liên lạc của tổ chức, cá nhân phụ trách của Bên chuyển dữ liệu c) Mô tả và luận giải mục tiêu của các hoạt động xử lý dữ liệu d) Mô tả và làm rõ loại dữ liệu đ) Mô tả và nêu rõ sự tuân thủ quy định bảo vệ dữ liệu, chi tiết các biện pháp bảo vệ dữ liệu e) Đánh giá mức độ ảnh hưởng của việc xử lý dữ liệu cá nhân; hậu quả, thiệt hại không mong muốn có khả năng xảy ra, các biện pháp giảm thiểu hoặc loại bỏ nguy cơ, tác hại đó; g) Sự đồng ý của chủ thể dữ liệu theo quy định tại Điều 11 Nghị định này trên cơ sở biết rõ cơ chế phản hồi, khiếu nại khi có sự cố hoặc yêu cầu phát sinh; h) Có văn bản thể hiện sự ràng buộc, trách nhiệm giữa các tổ chức, cá nhân chuyển và nhận dữ liệu cá nhân của Công dân Việt Nam về việc xử lý dữ liệu cá nhân.	**7.2.5 Đánh giá tác động quyền riêng tư** Tổ chức phải đánh giá sự cần thiết và thực hiện khi thích hợp, đánh giá tác động đến quyền riêng tư bất cứ khi nào việc xử lý PII mới hoặc các thay đổi đối với quá trình xử lý PII hiện tại được lên kế hoạch. **7.2.8 Hồ sơ liên quan đến xử lý PII** Tổ chức phải xác định và duy trì an toàn các hồ sơ cần thiết để hỗ trợ các nghĩa vụ của mình đối với việc xử lý PII. **7.5.3 Hồ sơ chuyển giao PII** Tổ chức phải ghi lại các chuyển giao PII đến hoặc từ các bên thứ ba và đảm bảo hợp tác với các bên đó để hỗ trợ các yêu cầu trong tương lai liên quan đến nghĩa vụ đối với các chủ thể PII.

Điều 25. Chuyển dữ liệu cá nhân ra nước ngoài	ISO/IEC 27701
3. Hồ sơ đánh giá tác động chuyển dữ liệu cá nhân ra nước ngoài phải luôn có sẵn để phục vụ hoạt động kiểm tra, đánh giá của Bộ Công an. Bên chuyển dữ liệu ra nước ngoài gửi 01 bản chính hồ sơ tới Bộ Công an (Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao) theo Mẫu số 06 tại Phụ lục của Nghị định này trong thời gian 60 ngày kể từ ngày tiến hành xử lý dữ liệu cá nhân.	Tiêu chuẩn ISO/IEC 27701 không yêu cầu cụ thể, áp dụng theo qui định của Luật
4. Bên chuyển dữ liệu thông báo gửi Bộ Công an (Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao) thông tin về việc chuyển dữ liệu và chi tiết liên lạc của tổ chức, cá nhân phụ trách bằng văn bản sau khi việc chuyển dữ liệu diễn ra thành công.	Tiêu chuẩn ISO/IEC 27701 không yêu cầu cụ thể, áp dụng theo qui định của Luật

Điều 25. Chuyển dữ liệu cá nhân ra nước ngoài	ISO/IEC 27701
5. Bộ Công an (Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao) đánh giá, yêu cầu Bên chuyển dữ liệu ra nước ngoài hoàn thiện Hồ sơ đánh giá tác động chuyển dữ liệu cá nhân ra nước ngoài trong trường hợp hồ sơ chưa đầy đủ và đúng quy định.	Tiêu chuẩn ISO/IEC 27701 không yêu cầu cụ thể, áp dụng theo qui định của Luật
6. Bên chuyển dữ liệu ra nước ngoài cập nhật, bổ sung Hồ sơ đánh giá tác động chuyển dữ liệu cá nhân ra nước ngoài khi có sự thay đổi về nội dung hồ sơ đã gửi cho Bộ Công an (Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao) theo Mẫu số 05 tại Phụ lục của Nghị định này. Thời gian hoàn thiện hồ sơ dành cho Bên chuyển dữ liệu ra nước ngoài là 10 ngày kể từ ngày yêu cầu.	Tiêu chuẩn ISO/IEC 27701 không yêu cầu cụ thể, áp dụng theo qui định của Luật

Điều 25. Chuyển dữ liệu cá nhân ra nước ngoài	ISO/IEC 27701
7. Căn cứ tình hình cụ thể, Bộ Công an quyết định việc kiểm tra chuyển dữ liệu cá nhân ra nước ngoài 01 lần/năm, trừ trường hợp phát hiện hành vi vi phạm quy định của pháp luật về bảo vệ dữ liệu cá nhân tại Nghị định này hoặc để xảy ra sự cố lộ, mất dữ liệu cá nhân của công dân Việt Nam.	Tiêu chuẩn ISO/IEC 27701 không yêu cầu cụ thể, áp dụng theo qui định của Luật
8. Bộ Công an quyết định yêu cầu Bên chuyển dữ liệu ra nước ngoài ngừng chuyển dữ liệu cá nhân ra nước ngoài trong trường hợp: a) Khi phát hiện dữ liệu cá nhân được chuyển được sử dụng vào hoạt động vi phạm lợi ích, an ninh quốc gia của nước Cộng hòa xã hội chủ nghĩa Việt Nam; b) Bên chuyển dữ liệu ra nước ngoài không chấp hành quy định tại khoản 5, khoản 6 Điều này; c) Để xảy ra sự cố lộ, mất dữ liệu cá nhân của công dân Việt Nam.	Tiêu chuẩn ISO/IEC 27701 không yêu cầu cụ thể, áp dụng theo qui định của Luật

Điều 28. Bảo vệ dữ liệu cá nhân nhạy cảm	ISO/IEC 27701
2. Chỉ định bộ phận có chức năng bảo vệ dữ liệu cá nhân, chỉ định nhân sự phụ trách bảo vệ dữ liệu cá nhân và trao đổi thông tin về bộ phận và cá nhân phụ trách bảo vệ dữ liệu cá nhân với Cơ quan chuyên trách bảo vệ dữ liệu cá nhân. Trường hợp Bên Kiểm soát dữ liệu cá nhân, Bên Kiểm soát và xử lý dữ liệu cá nhân, Bên Xử lý dữ liệu, Bên thứ ba là cá nhân thì trao đổi thông tin của cá nhân thực hiện.	**6.3.1.1 Vai trò và trách nhiệm an toàn thông tin** Tổ chức nên chỉ định một đầu mối liên hệ để khách hàng sử dụng liên quan đến việc xử lý PII. Khi tổ chức là bên kiểm soát PII, hãy chỉ định một đầu mối liên hệ cho các chủ thể về việc xử lý PII của họ (xem 7.3.2). Tổ chức nên chỉ định một hoặc nhiều người chịu trách nhiệm phát triển, thực hiện, duy trì và giám sát một chương trình quản trị và quyền riêng tư trong toàn tổ chức, để đảm bảo tuân thủ tất cả các luật và quy định hiện hành liên quan đến việc xử lý PII.

Điều 38. Trách nhiệm của Bên Kiểm soát dữ liệu cá nhân	ISO/IEC 27701
1. Thực hiện các biện pháp tổ chức và kỹ thuật cùng các biện pháp an toàn, bảo mật phù hợp để chứng minh các hoạt động xử lý dữ liệu đã được thực hiện theo quy định của pháp luật về bảo vệ dữ liệu cá nhân, rà soát và cập nhật các biện pháp này khi cần thiết.	**Áp dụng** - Hệ thống quản lý an toàn thông tin ISO/IEC 27001:2013 (ISO 27001:2022) - Hệ thống quản lý thông tin riêng tư ISO/IEC 27701:2019
2. Ghi lại và lưu trữ nhật ký hệ thống quá trình xử lý dữ liệu cá nhân.	**7.2.8 Hồ sơ liên quan đến xử lý PII** Tổ chức phải xác định và duy trì an toàn các hồ sơ cần thiết để hỗ trợ các nghĩa vụ của mình đối với việc xử lý PII.
3. Thông báo hành vi vi phạm quy định về bảo vệ dữ liệu cá nhân theo quy định tại Điều 23 Nghị định này.	**8.2.4 Hướng dẫn vi phạm** Tổ chức phải thông báo cho khách hàng nếu, theo quan điểm của mình, hướng dẫn xử lý vi phạm luật và/hoặc quy định hiện hành.
4. Lựa chọn Bên Xử lý dữ liệu cá nhân phù hợp với nhiệm vụ rõ ràng và chỉ làm việc với Bên Xử lý dữ liệu cá nhân có các biện pháp bảo vệ phù hợp.	**7.2.6 Hợp đồng với bên xử lý PII** Tổ chức phải có hợp đồng bằng văn bản với bất kỳ đơn vị xử lý PII nào mà tổ chức sử dụng và phải đảm bảo rằng hợp đồng với các đơn vị xử lý PII đề cập đến việc thực hiện các biện pháp kiểm soát thích hợp trong Phụ lục B.

Điều 38. Trách nhiệm của Bên Kiểm soát dữ liệu cá nhân	ISO/IEC 27701
5. Bảo đảm các quyền của chủ thể dữ liệu theo quy định tại Điều 9 Nghị định này	**Áp dụng** - Hệ thống quản lý an toàn thông tin ISO/IEC 27001:2013 (ISO 27001:2022) - Hệ thống quản lý thông tin riêng tư ISO/IEC 27701:2019
6. Bên Kiểm soát dữ liệu cá nhân chịu trách nhiệm trước chủ thể dữ liệu về các thiệt hại do quá trình xử lý dữ liệu cá nhân gây ra.	Tiêu chuẩn ISO/IEC 27701 không yêu cầu cụ thể, áp dụng theo qui định của Luật
7. Phối hợp với Bộ Công an, cơ quan nhà nước có thẩm quyền trong bảo vệ dữ liệu cá nhân, cung cấp thông tin phục vụ điều tra, xử lý hành vi vi phạm quy định của pháp luật về bảo vệ dữ liệu cá nhân.	Tiêu chuẩn ISO/IEC 27701 không yêu cầu cụ thể, áp dụng theo qui định của Luật

Điều 39. Trách nhiệm của Bên Xử lý dữ liệu cá nhân	
1. Chỉ tiếp nhận dữ liệu cá nhân sau khi có hợp đồng hoặc thỏa thuận về xử lý dữ liệu với Bên Kiểm soát dữ liệu cá nhân.	**8.2.1 Sự đồng ý của khách hàng** Tổ chức phải đảm bảo, nếu có liên quan, hợp đồng xử lý PII đề cập đến vai trò của tổ chức trong việc hỗ trợ các nghĩa vụ của khách hàng, (có tính đến bản chất của quá trình xử lý và thông tin có sẵn cho tổ chức).
2. Xử lý dữ liệu cá nhân theo đúng hợp đồng hoặc thỏa thuận ký kết với Bên Kiểm soát dữ liệu cá nhân.	**8.2.2 Mục đích của tổ chức** Tổ chức phải đảm bảo rằng PII được xử lý thay mặt cho khách hàng chỉ được xử lý cho các mục đích được thể hiện trong các hướng dẫn bằng văn bản của khách hàng.
3. Thực hiện đầy đủ các biện pháp bảo vệ dữ liệu cá nhân quy định tại Nghị định này và các văn bản pháp luật khác có liên quan.	**Áp dụng** - Hệ thống quản lý an toàn thông tin ISO/IEC 27001:2013 (ISO 27001:2022) - Hệ thống quản lý thông tin riêng tư ISO/IEC 27701:2019

Điều 39. Trách nhiệm của Bên Xử lý dữ liệu cá nhân	
4. Bên Xử lý dữ liệu cá nhân chịu trách nhiệm trước chủ thể dữ liệu về các thiệt hại do quá trình xử lý dữ liệu cá nhân gây ra.	**8.3.1 Nghĩa vụ đối với các chủ thể PII** Tổ chức phải cung cấp cho khách hàng các phương tiện để thực hiện các nghĩa vụ của mình liên quan đến các chủ thể PII.
5. Xóa, trả lại toàn bộ dữ liệu cá nhân cho Bên Kiểm soát dữ liệu cá nhân sau khi kết thúc xử lý dữ liệu.	**8.4.2 Trả lại, chuyển giao hoặc loại bỏ PII** Tổ chức phải cung cấp khả năng trả lại, chuyển giao và / hoặc loại bỏ PII một cách an toàn. Chính sách cũng phải có sẵn cho khách hàng.
6. Phối hợp với Bộ Công an, cơ quan nhà nước có thẩm quyền trong bảo vệ dữ liệu cá nhân, cung cấp thông tin phục vụ điều tra, xử lý hành vi vi phạm quy định của pháp luật về bảo vệ dữ liệu cá nhân.	Tiêu chuẩn ISO/IEC 27701 không yêu cầu cụ thể, áp dụng theo qui định của Luật

Điều 40. Trách nhiệm của Bên Kiểm soát và xử lý dữ liệu	
Thực hiện đầy đủ các quy định về trách nhiệm của Bên Kiểm soát dữ liệu cá nhân và Bên Xử lý dữ liệu cá nhân.	

Chứng nhận ISO/IEC 27701

Là …

- Hệ thống quản lý thông tin quyền riêg tư - Privacy Information Management System (PIMS)
- Tiêu chuẩn không bao gồm luật cụ thể cung cấp sự tin tưởng rằng riêng tư được quản lý
- Có thể giúp chứng minh việc quản lý PII theo bất kỳ luật nào

Không bao gồm…

- Chứng nhận theo bất kỳ luật cụ thể nào

Chứng nhận theo ISO/IEC 27701 với BSI sẽ bao gồm...

- **Đánh giá GAP (tùy chọn)**

  Đánh giá sơ bộ để biết mức độ đáp ứng các yêu cầu trước cuộc đánh giá chính thức

- **Đánh giá chính thức**

  Đây là một quá trình gồm hai giai đoạn để đảm bảo PIMS của bạn đang hoạt động hiệu quả theo các yêu cầu chứng nhận ISO/IEC 27701. Thời lượng khác nhau tùy thuộc vào số lượng và loại PII mà tổ chức của bạn phải chịu trách nhiệm

- **Đánh giá giám sát**

  Cuộc đánh giá định kỳ hàng năm để đảm bảo giá trị gia tăng cho PIMS của bạn.

Vì sao nên chọn BSI đánh giá ISO/IEC 27701?

- BSI là tổ chức tiên phong trong các tiêu chuẩn an toàn thông tin từ năm 1995
- BSI đưa ra tiêu chuẩn đầu tiên trên thế giới - BS 7799, nay là ISO/IEC 27001 - tiêu chuẩn an toàn thông tin phổ biến nhất thế giới
- BSI luôn đi đầu trong việc giải quyết các vấn đề mới như An toàn thông tin, bảo vệ quyền riêng tư, bảo vệ dữ liệu các nhân,..
- Chúng tôi có bí quyết kỹ thuật và mạng lưới để thúc đẩy chương trình chứng nhận về bảo vệ quyền riêng tư và dữ liệu cá nhân cho các tổ chức và doanh nghiệp.

CÂU HỎI VÀ TRẢ LỜI

TO SHARE KNOWLEDGE, INNOVATION AND BEST PRACTICE TO HELP PEOPLE AND ORGANIZATIONS REALIZE THEIR POTENTIAL AND MAKE EXCELLENCE A HABIT

Xin cám ơn Quý Anh/ Chị đã xem tham dự hội thảo được tổ chức bởi BSI Việt Nam

Liên hệ hoặc quét mã QR để tìm hiểu thêm:

Viện tiêu chuẩn Anh - BSI Việt Nam

Trụ sở chính: Tầng 15, Tòa nhà AP, 518B Điện Biên Phủ, Phường 21, Quận Bình Thạnh, Thành phố Hồ Chính Minh

T: +84 (28) 3820 0066

F: +84 (28) 3820 0022

Info.Vietnam@bsigroup.com | www.bsigroup.com

Văn phòng Hà Nội: Tầng 12, Tòa nhà PV Oil, 148 Hoàng Quốc Việt, Phường Nghĩa Tân, Quận Cầu Giấy, Thủ Đô Hà Nội

T: +84 (24) 3762 1170

F: +84 (24) 3762 1171

Info.Hanoi@bsigroup.com | www.bsigroup.com

Văn phòng Đà Nẵng: Lô G, Tầng 8, Công viên phần mềm Đà Nẵng, 02 Quang Trung, Quận Hải Châu Thành phố Đà Nẵng

T: +84 (23) 6388 8468

F: +84 (23) 6388 8719

VanBac.Doan@bsigroup.com | www.bsigroup.com

bsi.