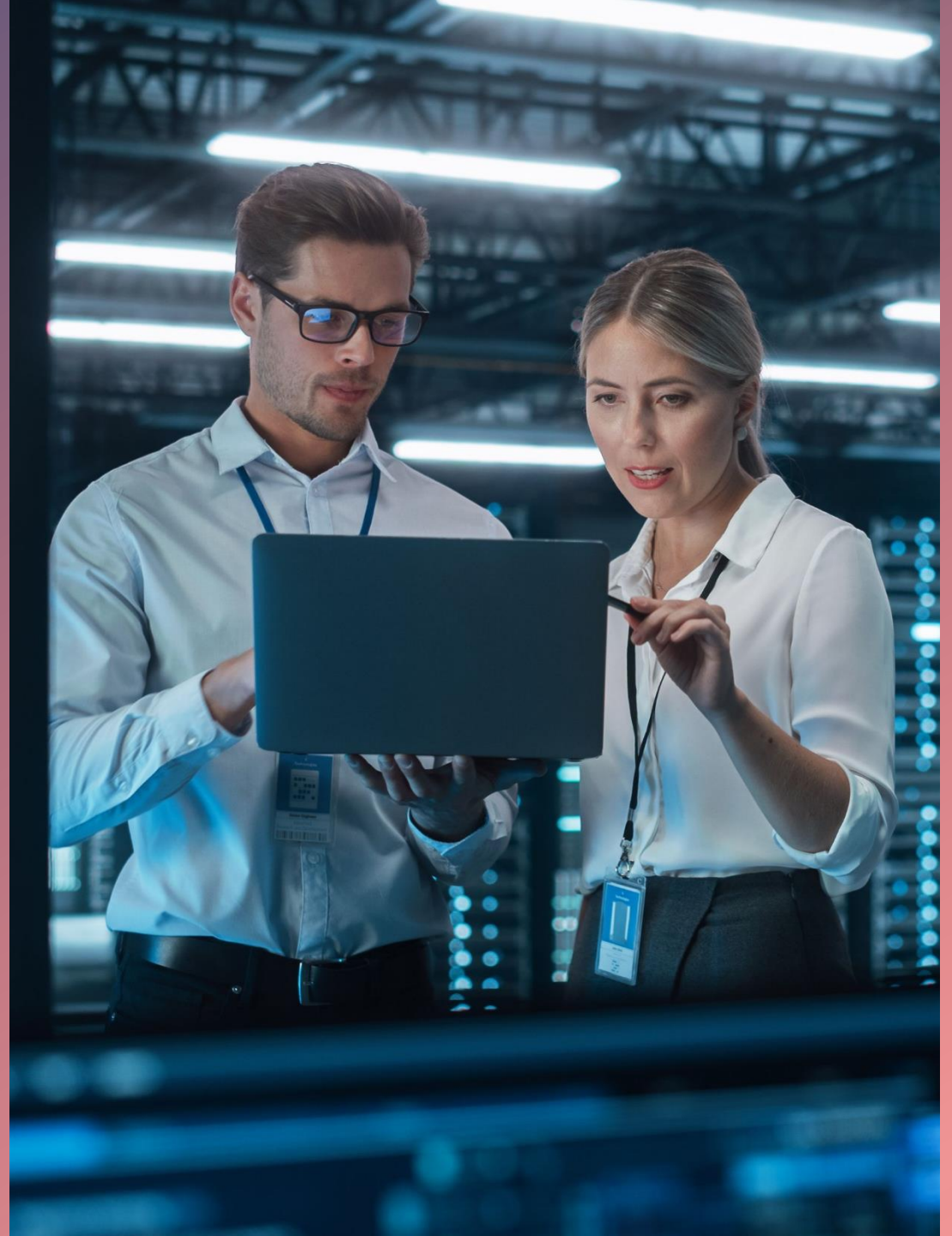
ความสัมพันธ์ระหว่าง พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA) และ ISO/IEC 27701

BSI Group (Thailand)



หัวข้อชวนคุย

1. ภาพรวมพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล
2. ภาพรวมมาตรฐาน ISO/IEC 27701
3. ข้อกำหนดมาตรฐาน ISO/IEC 27701 กับการดำเนินการตาม พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
4. Certify ISO/IEC 27701
5. ผลกระทบ ของ การปรับเปลี่ยน ISO/IEC 27001:2022

bsi.

ภาพรวมพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (Personal Data Protection Act – PDPA) พ.ศ. 2562 รวมถึงมาตรฐานที่เกี่ยวข้องอื่นๆ

เหตุผลในการประกาศใช้พระราชบัญญัติฉบับนี้

เนื่องจากปัจจุบัน**มีการล่วงละเมิด สิทธิความเป็นส่วนตัวของข้อมูลส่วนบุคคลเป็นจำนวนมาก**จนสร้าง**ความเดือดร้อนรำคาญหรือความเสียหาย** ให้แก่เจ้าของข้อมูลส่วนบุคคล

ความก้าวหน้าของเทคโนโลยีทำให้การเก็บรวบรวม ใช้ หรือ เปิดเผยข้อมูลส่วนบุคคลอันเป็นการล่วงละเมิดดังกล่าว ทำได้โดยง่าย สะดวก และรวดเร็ว

ก่อให้เกิด ความเสียหายต่อเศรษฐกิจโดยรวม

bsi.

คำศัพท์ต่างๆที่ควรรู้ เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล

“ข้อมูลส่วนบุคคล” หมายความว่า ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ

“ผู้ควบคุมข้อมูลส่วนบุคคล” หมายความว่า บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล/ Controller

“ผู้ประมวลผลข้อมูลส่วนบุคคล” หมายความว่า บุคคลหรือนิติบุคคลซึ่งดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล ทั้งนี้ บุคคลหรือนิติบุคคลซึ่งดำเนินการดังกล่าวไม่เป็นผู้ควบคุมข้อมูลส่วนบุคคล/ Processor

Noted: มาตรา ๖

bsi.

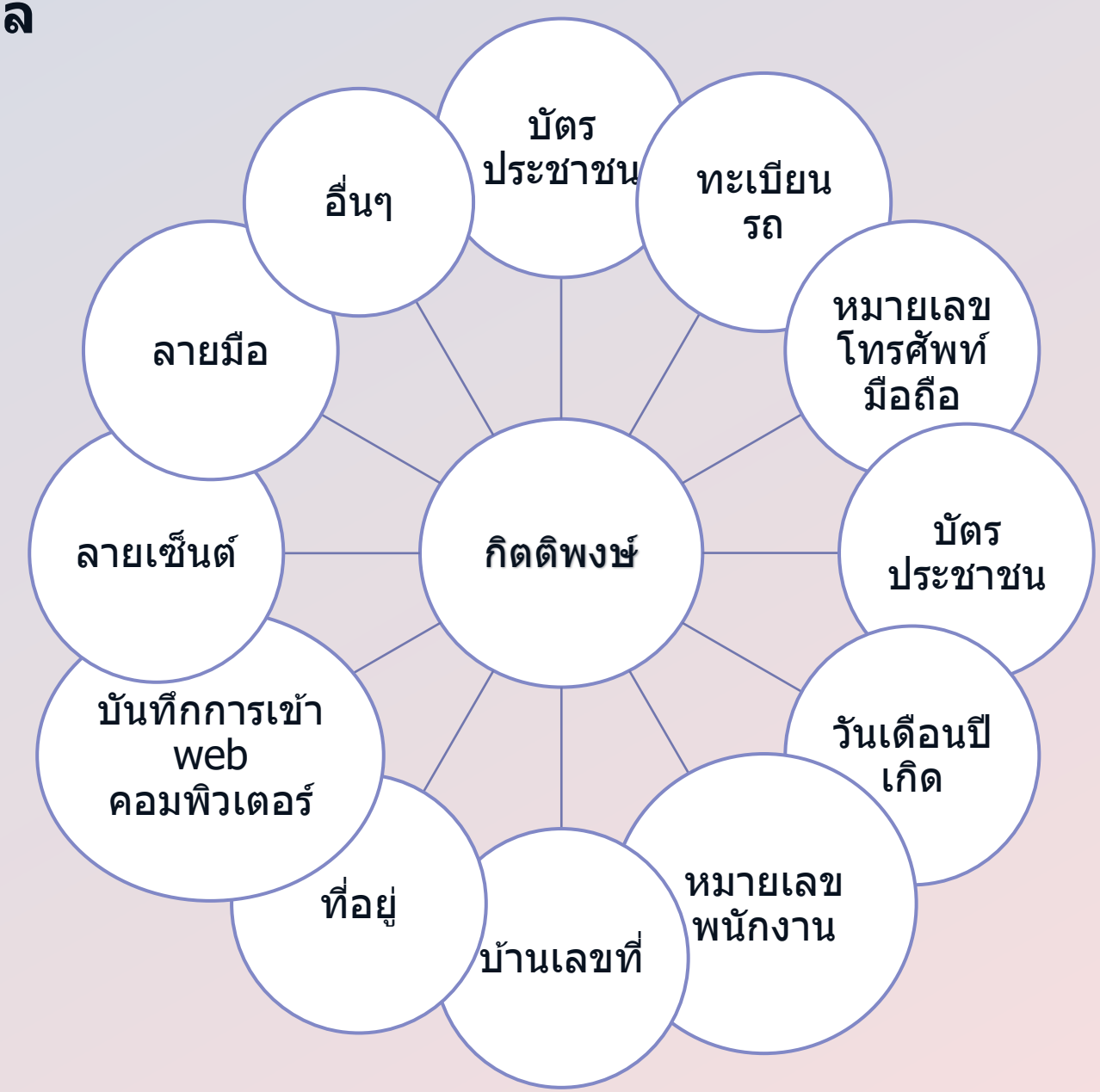
คำศัพท์ต่างๆที่ควรรู้ เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล

การประมวลผลข้อมูลส่วนบุคคล:

- การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูล ส่วนบุคคล (พระราชบัญญัติคุ้มครองข้อมูลส่วน บุคคล)

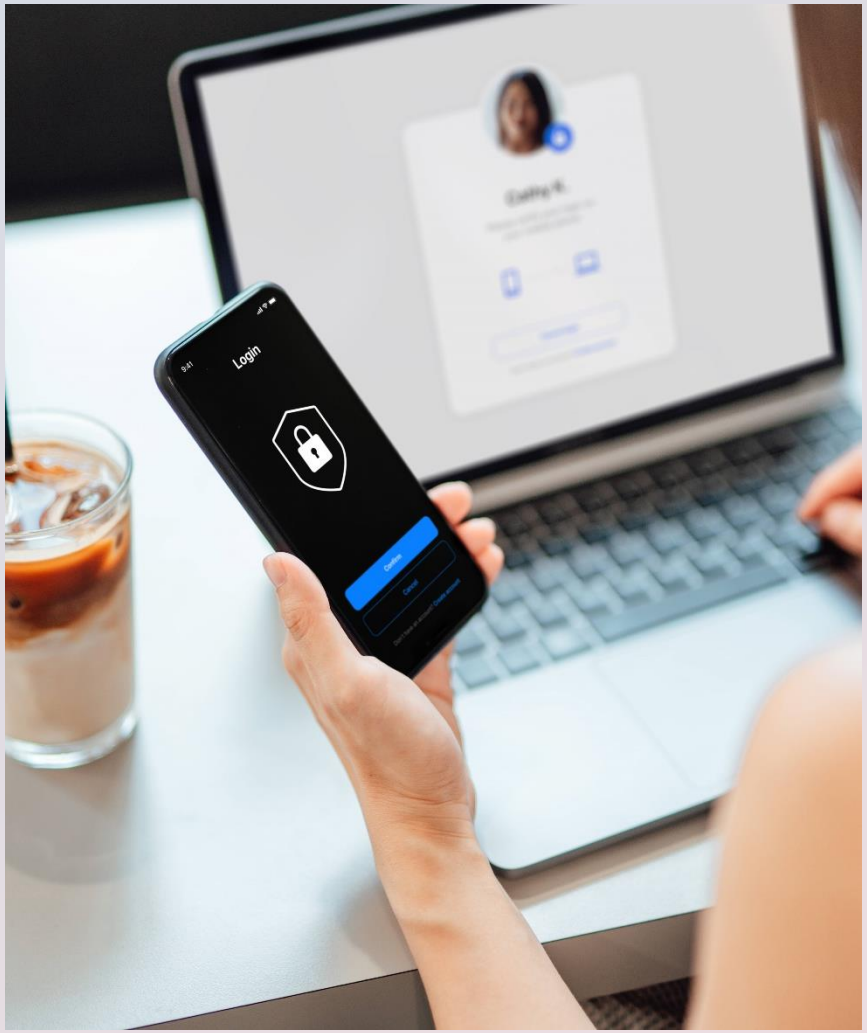
- การดำเนินการใดๆ หรือชุดของการดำเนินการที่กระทำกับข้อมูลส่วนบุคคลหรือชุดของข้อมูลส่วนบุคคล โดยวิธีการแบบอัตโนมัติหรือไม่ก็ตาม เช่นการรวบรวม การบันทึก การจัดการอย่างเป็นระบบ การจัดโครงสร้าง การจัดเก็บ การปรับเปลี่ยนหรือดัดแปลง การค้นคืนการให้คำปรึกษา การใช้งาน การเปิดเผยโดยการส่งผ่าน การเผยแพรหรือทำให้พร้อมใช้งาน การทำให้สอดคล้องหรือนำไปรวม การกำจัด การลบ หรือทำลาย *(GDPR Article 4 Definition)*

ข้อมูลส่วนบุคคล



bsi.

ข้อมูลส่วนบุคคล – พิเศษ



- เชื้อชาติ เผ่าพันธุ์
- ความคิดเห็นทางการเมือง
- ความเชื่อในลัทธิ ศาสนาหรือปรัชญา
- พฤติกรรมทางเพศ
- ประวัติอาชญากรรม
- ข้อมูลสุขภาพ ความพิการ
- ข้อมูลสหภาพแรงงาน
- ข้อมูลพันธุกรรม ข้อมูลชีวภาพ
- หรือข้อมูลอื่นใดซึ่งกระทบต่อเจ้าของข้อมูลส่วนบุคคลในทำนองเดียวกัน

Noted: *มาตรา ๒๖*

bsi.

ผู้ควบคุมข้อมูล

มหาวิทยาลัย

หน่วยงานภาครัฐ

ธนาคาร

Sport Club

บ. บัตรเครดิต

บ.ประกัน

โรงพยาบาล

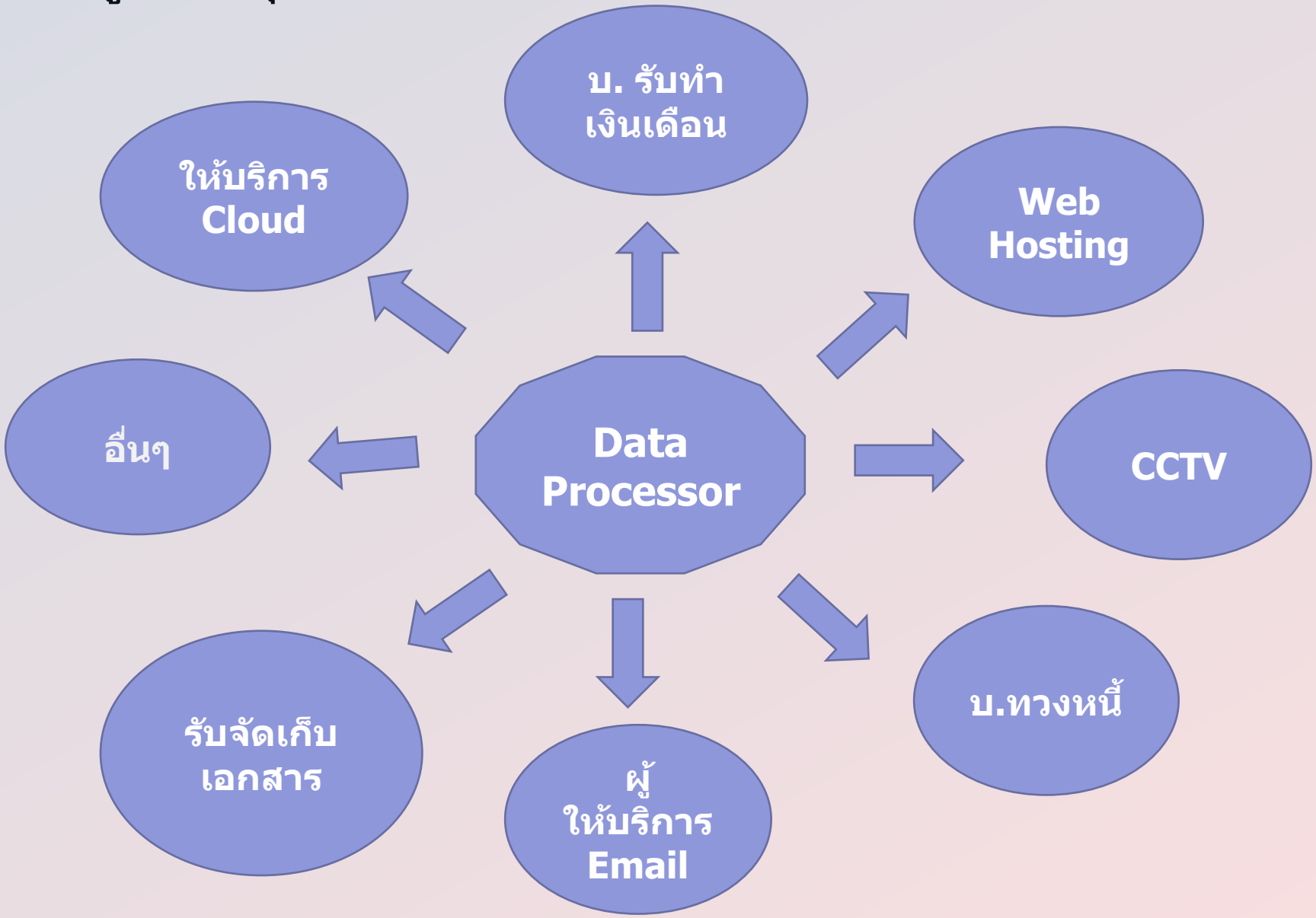
บ. จัดหางาน

ร้านขายของ

อื่นๆ

bsi.

ผู้ประมวลผลข้อมูลส่วนบุคคล



ฐานทางกฎหมาย

เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล

เป็นการจำเป็นเพื่อการปฏิบัติตามสัญญา

เพื่อประโยชน์สาธารณะ

การจำเป็นประโยชน์โดยชอบด้วยกฎหมาย

ปฏิบัติตามกฎหมาย

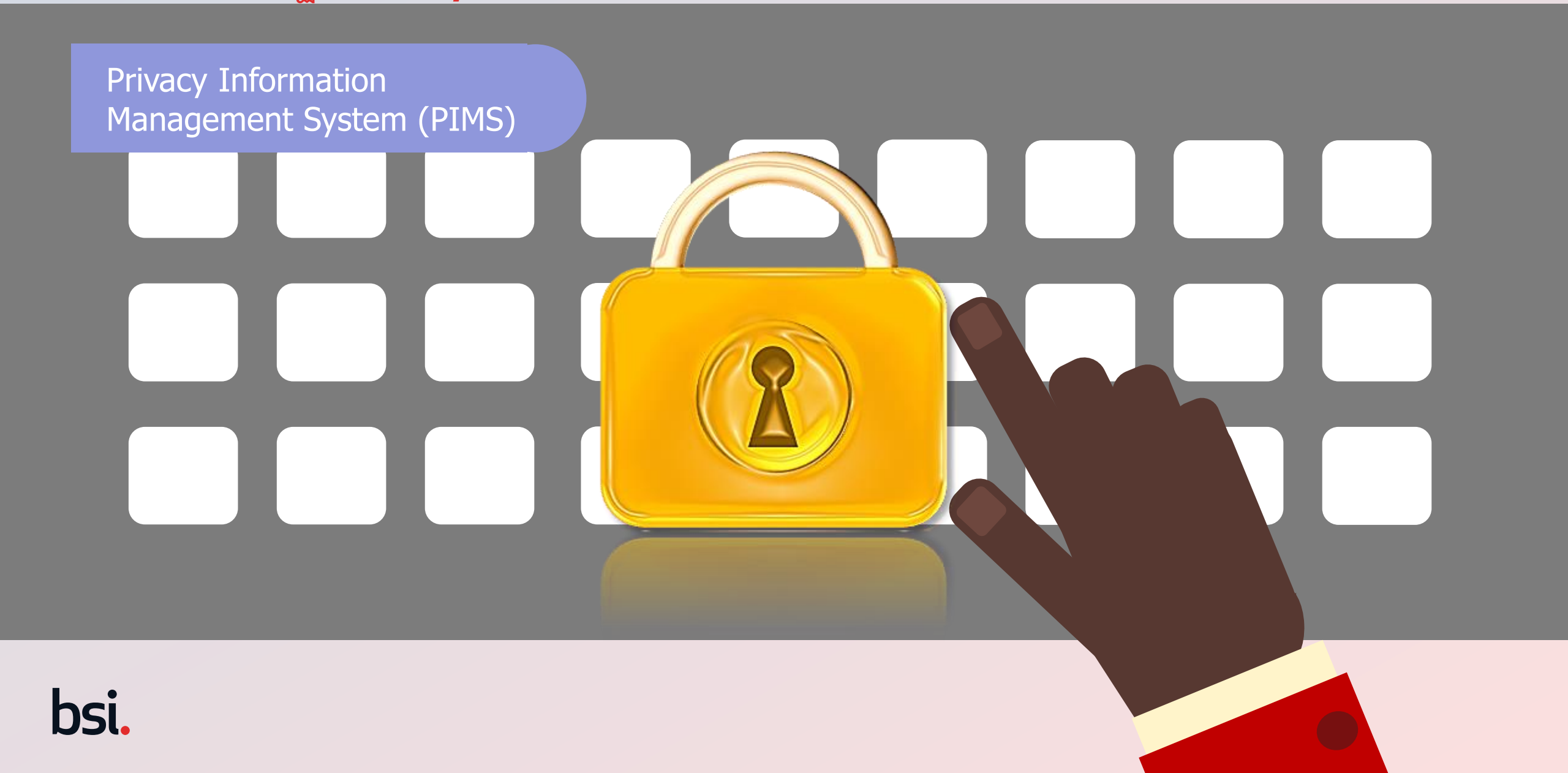
ได้รับความยินยอมจากเจ้าของข้อมูล

การจัดทำเอกสารประวัติศาสตร์หรือจดหมายเหตุ

bsi.

ภาพรวมมาตรฐาน ISO/IEC 27701

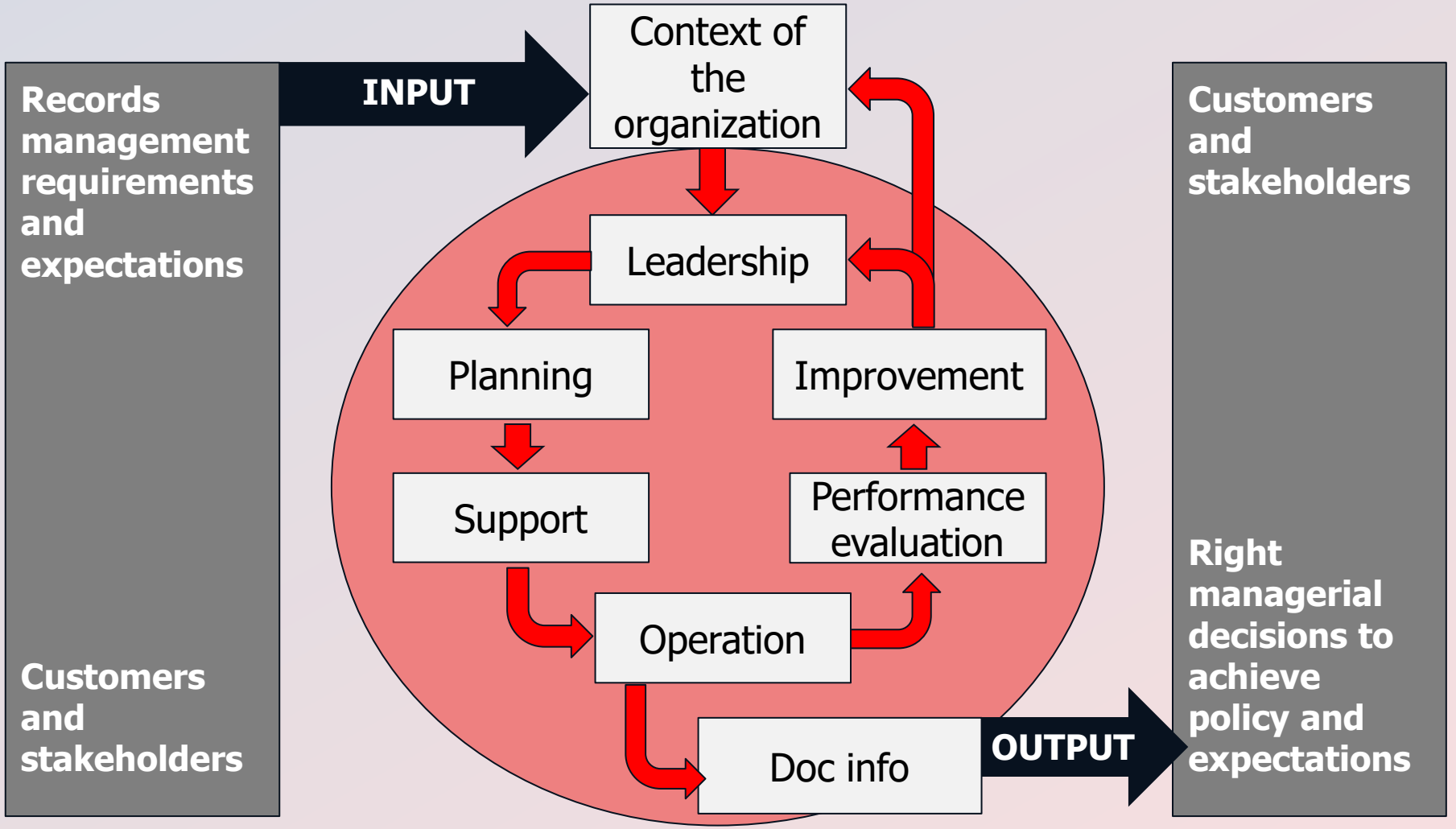
Privacy Information Management System (PIMS)

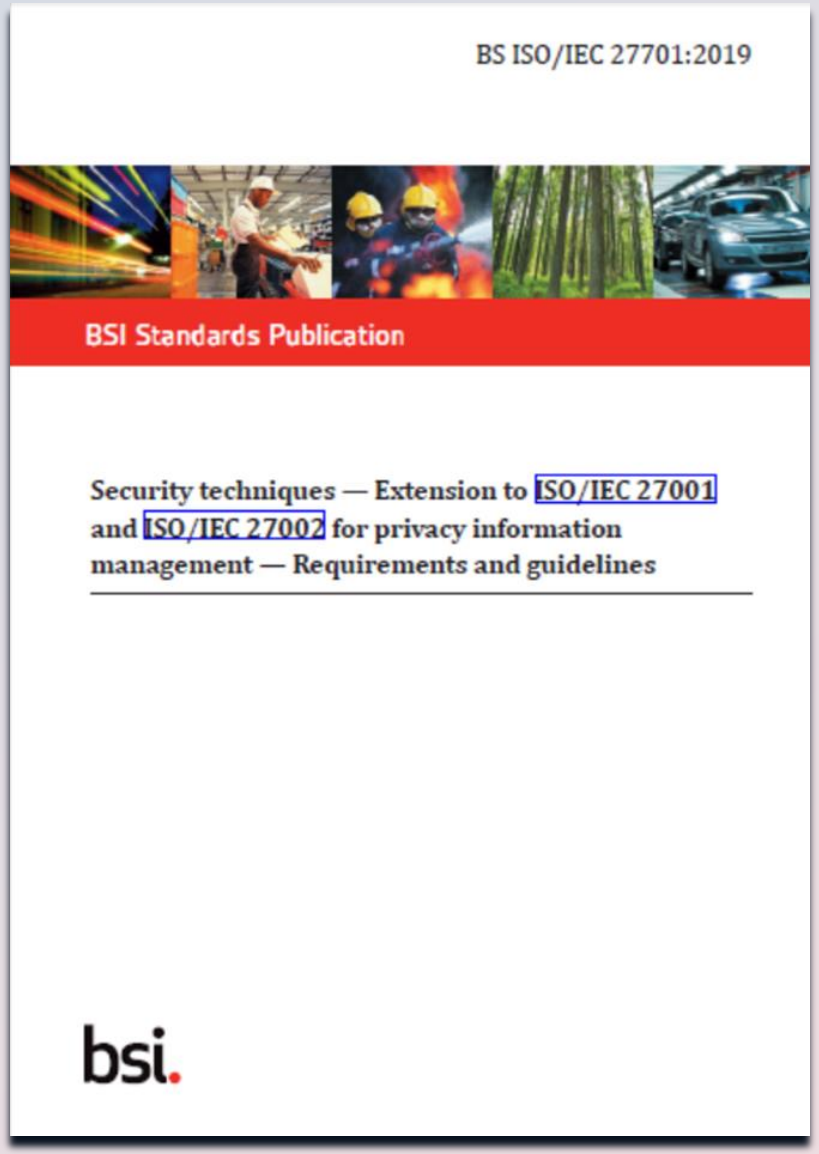


bsi.

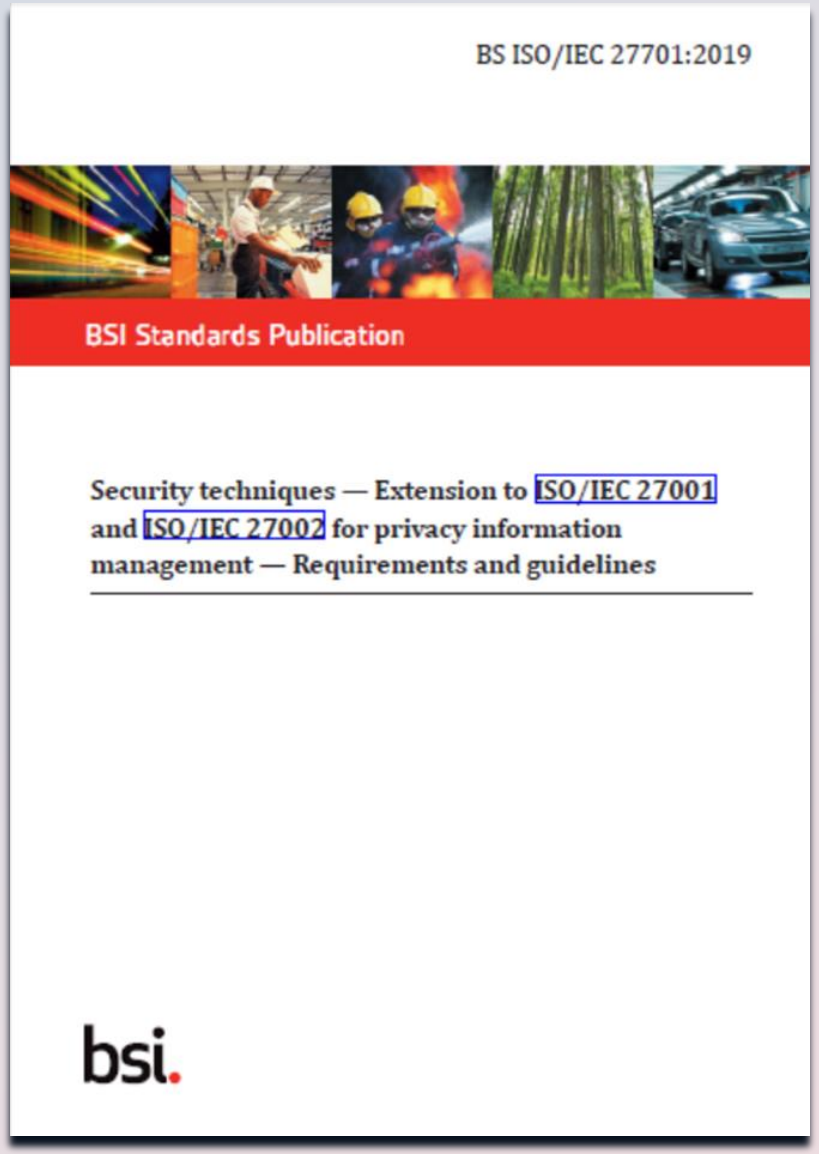
PIMS Plan, Do, Check, Act cycle

Integration – High level structure





Contents in ISO/IEC 27701



1. Scope
2. Normative Reference
3. Terms, definitions and abbreviations

4 General

Table 1 — Location of PIMS-specific requirements and other information for implementing controls in ISO/IEC 27001:2013

Clause in ISO/IEC 27001:2013	Title	Subclause in this document	Remarks
4	Context of the organization	5.2	Additional requirements
5	Leadership	5.3	No PIMS-specific requirements
6	Planning	5.4	Additional requirements
7	Support	5.5	No PIMS-specific requirements
8	Operation	5.6	No PIMS-specific requirements
9	Performance evaluation	5.7	No PIMS-specific requirements
10	Improvement	5.8	No PIMS-specific requirements

NOTE The extended interpretation of "information security" according to 5.1 always applies even when there are no PIMS-specific requirements.

4 General

Table 2 gives the location of PIMS-specific guidance in this document in relation to ISO/IEC 27002.

Table 2 — Location of PIMS-specific guidance and other information for implementing controls in ISO/IEC 27002:2013

Clause in ISO/IEC 27002:2013	Title	Subclause in this document	Remarks
5	Information security policies	6.2	Additional guidance
6	Organization of information security	6.3	Additional guidance
7	Human resource security	6.4	Additional guidance
8	Asset management	6.5	Additional guidance
9	Access control	6.6	Additional guidance
10	Cryptography	6.7	Additional guidance
11	Physical and environmental security	6.8	Additional guidance
12	Operations security	6.9	Additional guidance
13	Communications security	6.10	Additional guidance
14	System acquisition, development and maintenance	6.11	Additional guidance
15	Supplier relationships	6.12	Additional guidance
16	Information security incident management	6.13	Additional guidance
17	Information security aspects of business continuity management.	6.14	No PIMS-specific guidance
18	Compliance	6.15	Additional guidance

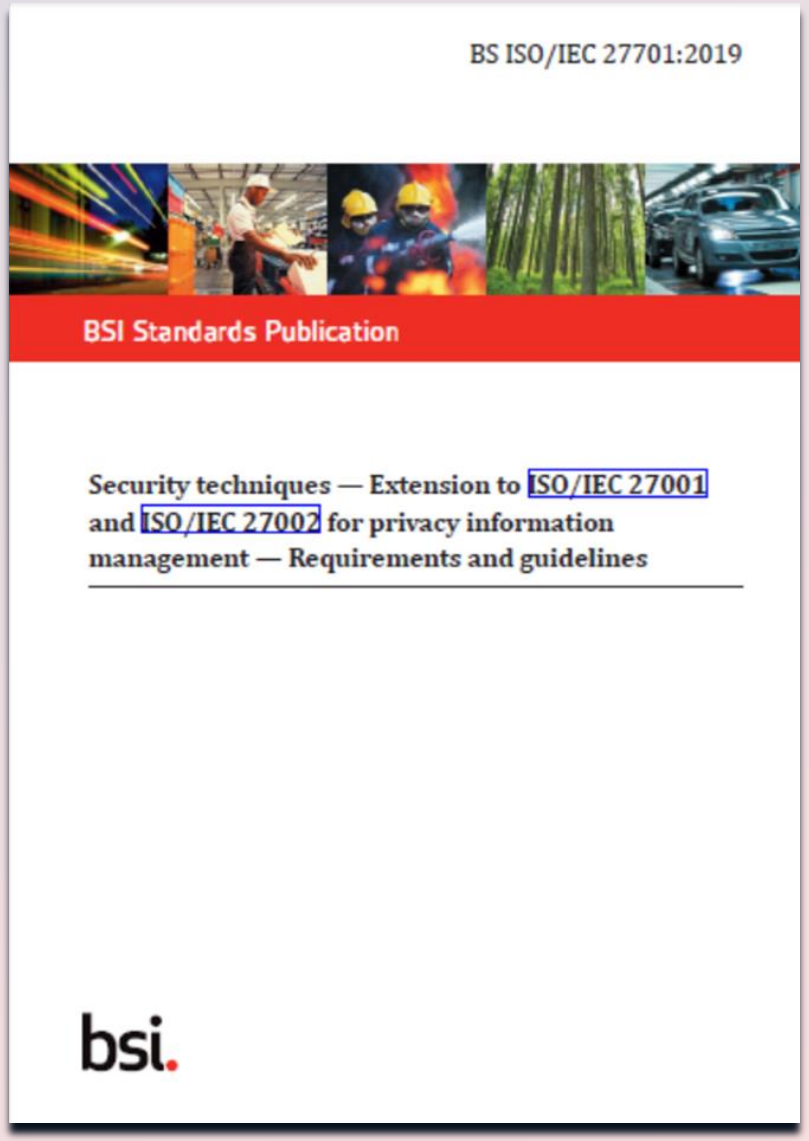
NOTE The extended interpretation of "information security" according to 6.1 always applies even when there is no PIMS-specific guidance.

Clause 5: PIMS-specific requirements related to ISO/IEC 27001

Clause 6: PIMS-specific guidance related to ISO/IEC 27002

Clause 7: Additional ISO/IEC 27002 guidance for PII controllers

Clause 8: Additional ISO/IEC 27002 guidance for PII processors



Annex A- F

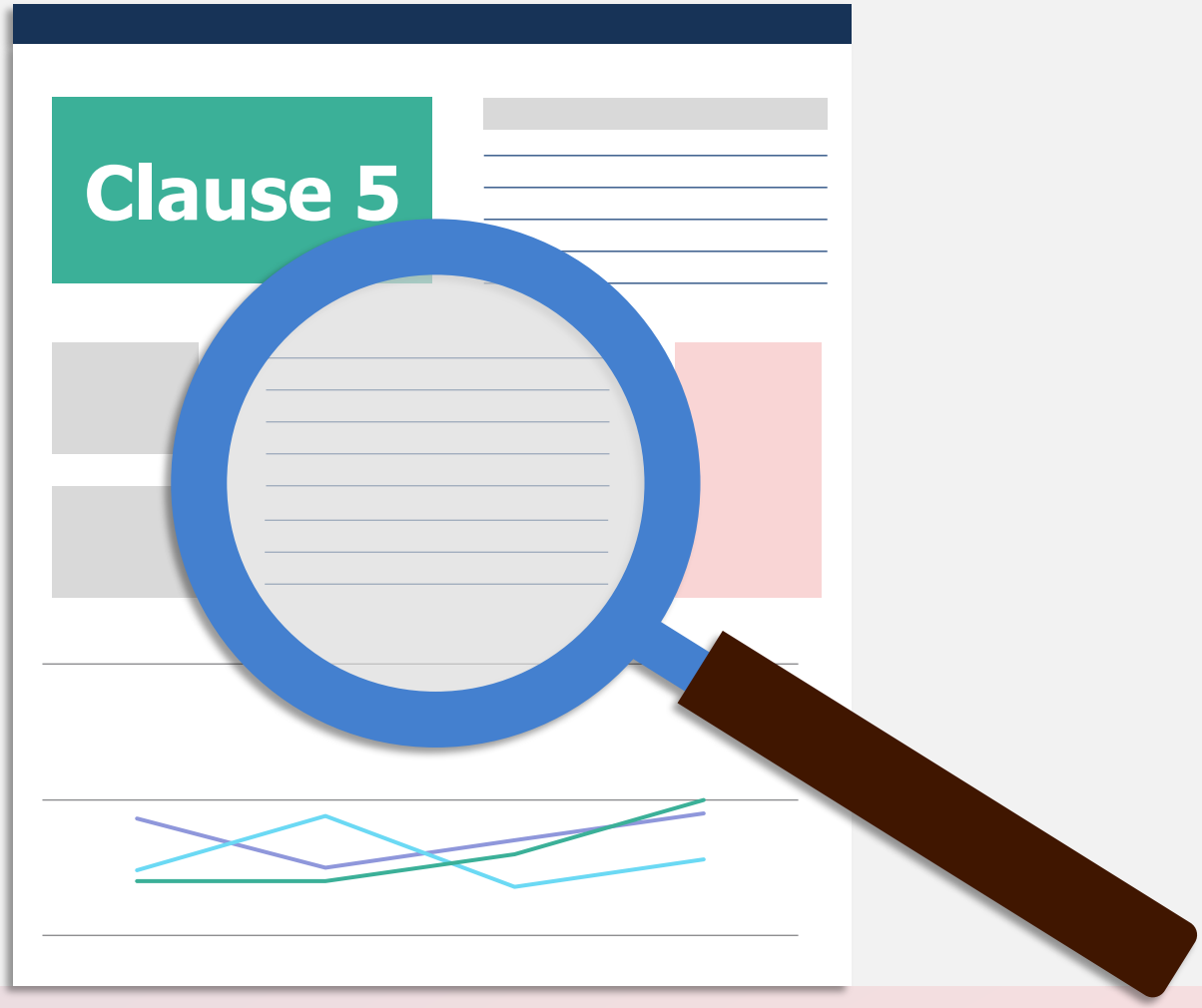
Annex	Detail
Annex A (informative)	PIMS-specific reference control objectives and controls (**PII Controllers**)
Annex B (normative)	PIMS-specific reference control objectives and controls (**PII Processors**)
Annex C (informative)	Mapping to ISO/IEC 29100 Table C.1 — Mapping of controls for **PII controllers** and ISO/IEC 29100 Table C.2 — Mapping of controls for **PII processors** and ISO/IEC 29100
Annex D (informative)	Mapping to the **General Data Protection Regulation**
Annex E (informative)	Mapping to ISO/IEC 27018 and ISO/IEC 29151
Annex F (informative)	How to apply ISO/IEC 27701 to ISO/IEC 27001 and ISO/IEC 27002

bsi.

ข้อกำหนดมาตรฐาน ISO/IEC 27701 กับการดำเนินการตาม พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

bsi.

Clause 5: PIMS-specific requirements related to ISO/IEC 27001



PIMS Plan, Do, Check, Act cycle

Clause 6: PIMS-specific requirements related to ISO 27002

Clause 6.1: General

Clause 6.2.1 and Clause 6.2.1.2

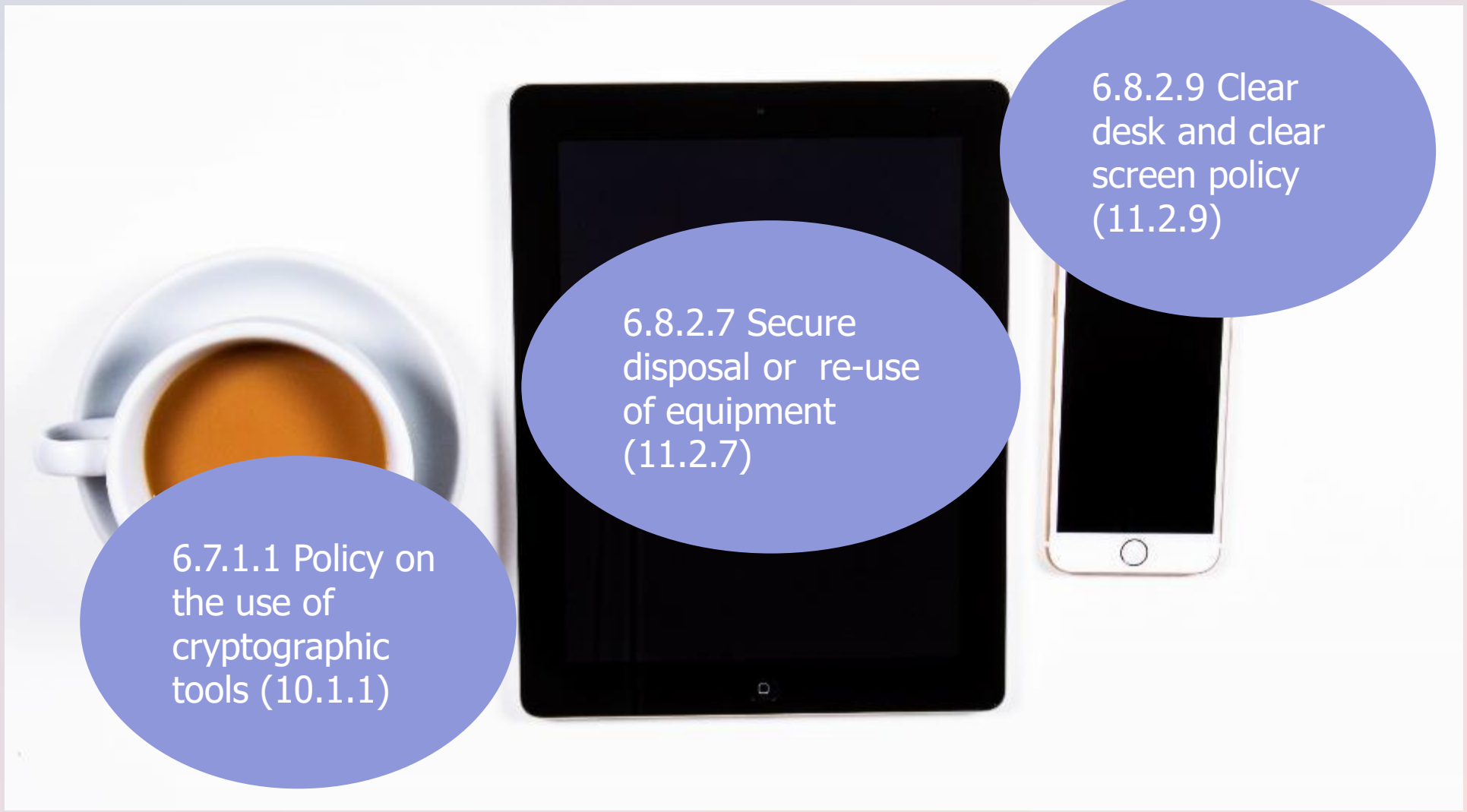
Clauses 6.3.1.1, 6.3.2.1, 6.4.2.2, 6.5.2.1, 6.5.2.2, 6.5.3.1, 6.5.3.2 and 6.5.3.3

- 6.3.1.1 Information security roles and responsibilities
- 6.3.2.1 Mobile device policy
- 6.4.2.2 Information security awareness, education and training
- 6.5.2.1 Classification of information
- 6.5.2.2 Labelling of information
- 6.5.3.1 Management of removable media
- 6.5.3.2 Disposal of media
- 6.5.3.3 Physical media transfer

Clause 6.6.2.1, Clause 6.6.2.2 and Clause 6.6.4.2

- 6.6.2.1 User registration and de-registration (9.2.1)
- 6.6.2.2 User access provisioning (9.2.2)
- 6.6.4.2 Secure log-on procedures (9.4.2)

Clause 6.7.1, Clause 6.8.2.7 and Clause 6.8.2.9

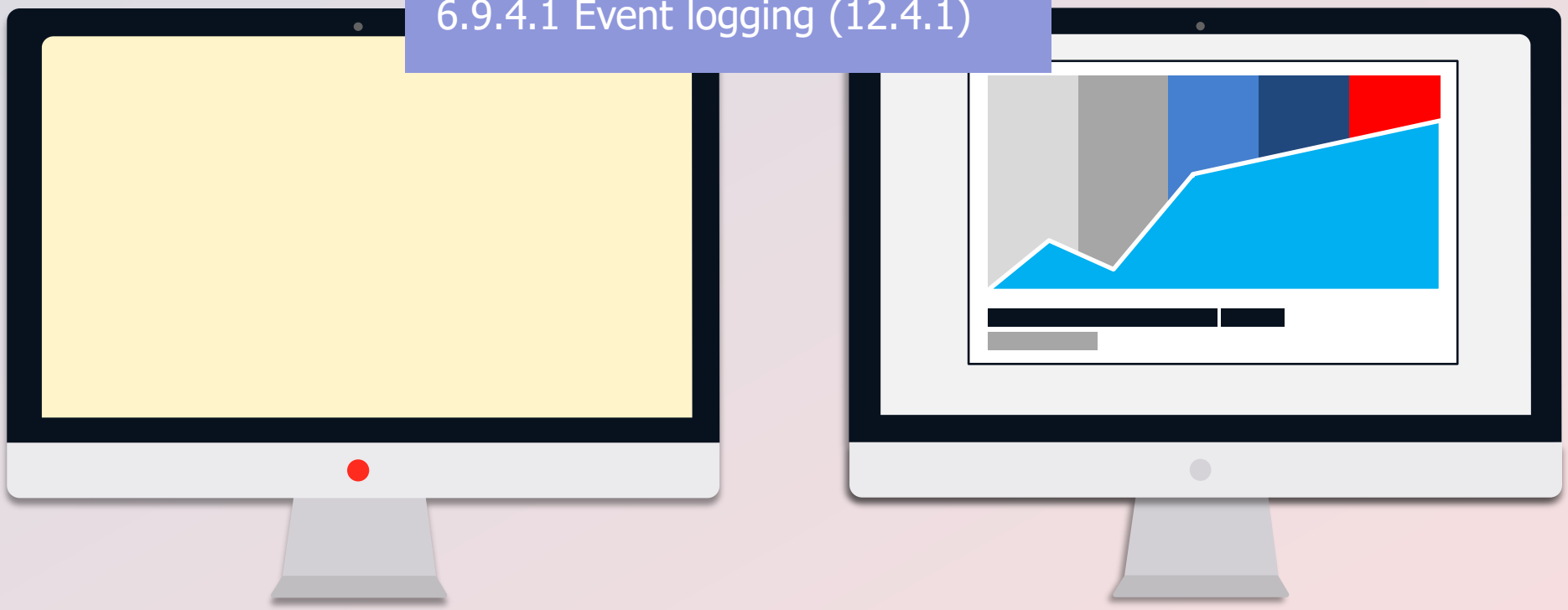


Clause 6.9.3.1, Clause 6.9.4.1 and Clause 6.9.4.2

6.9.3.1 Information backup (12.3.1)

6.9.4.2 Protection of log information (12.4.2)

6.9.4.1 Event logging (12.4.1)



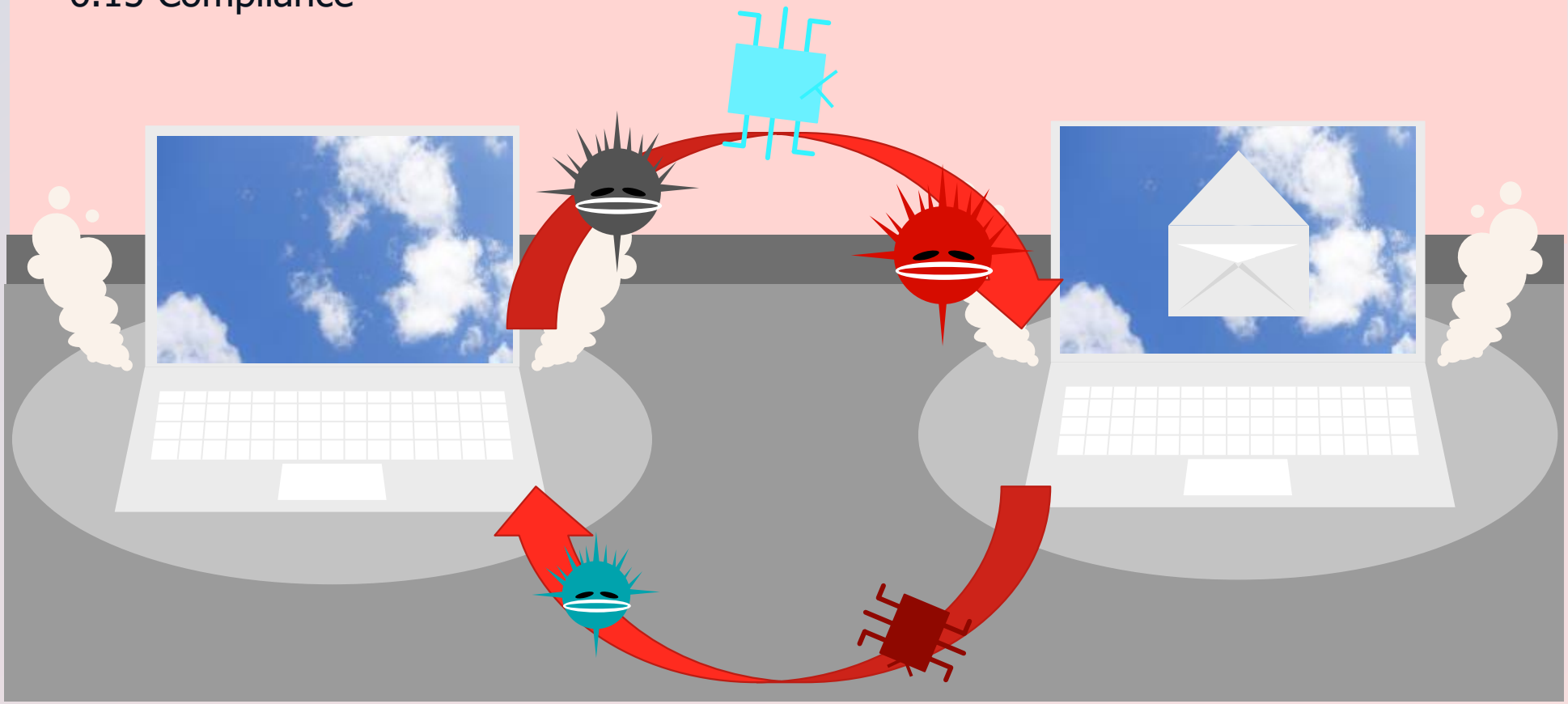
Clause 6.10 and Clause 6.11 subclauses

Clause 6.12.1.2 Addressing security within supplier agreements

Clause 6.13 and Clause 6.15 subclauses

6.13 Information security incident management

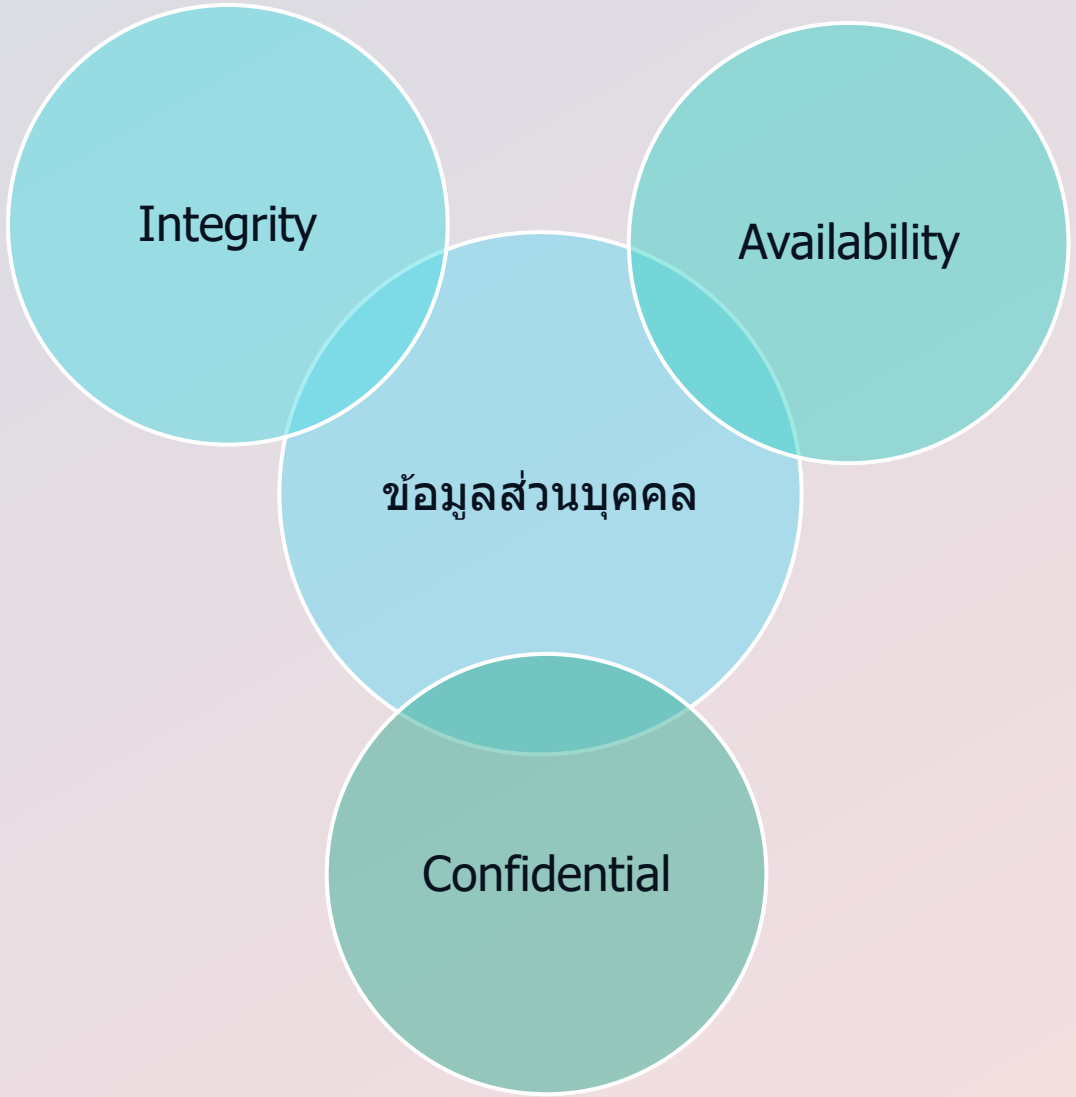
6.15 Compliance

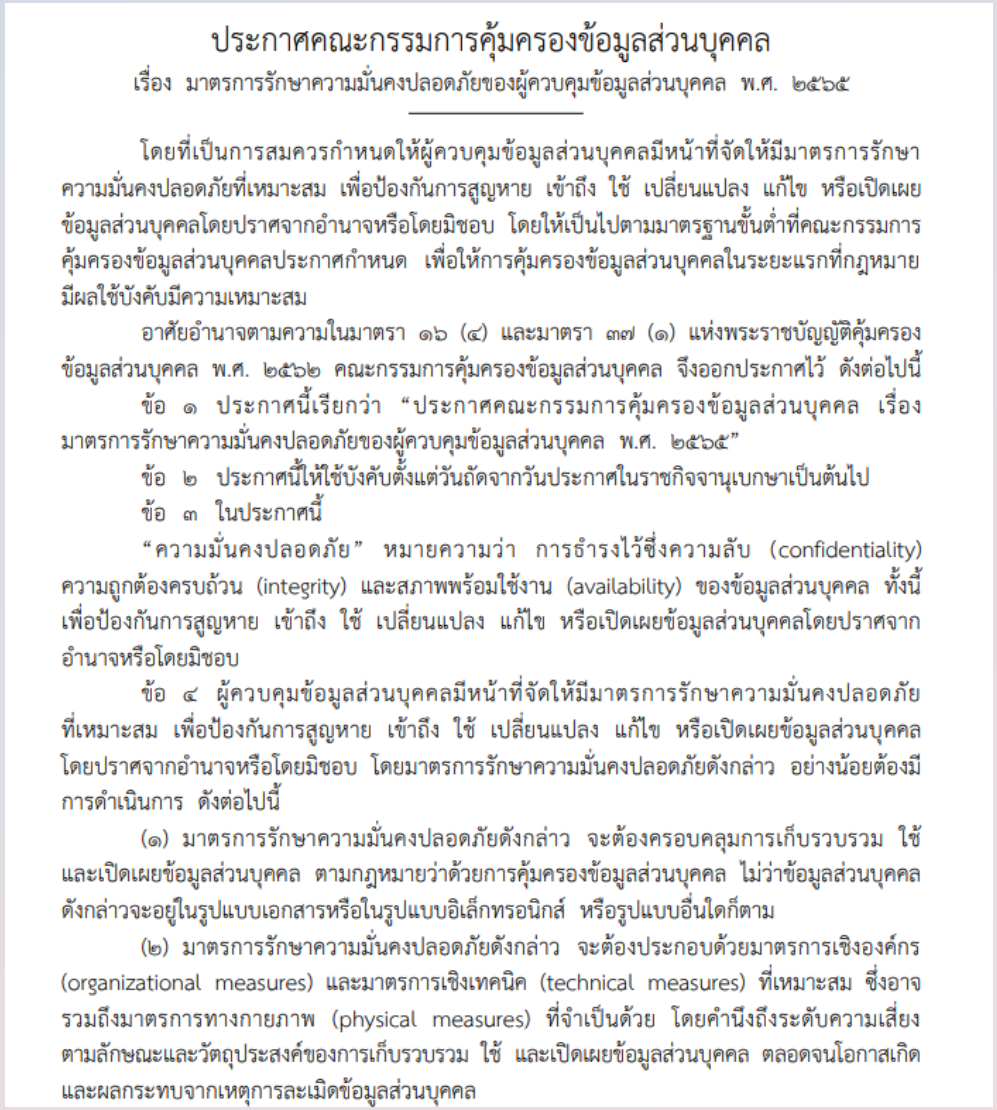


Summary Clause 6

Technical control for PII
- Security and privacy control

Summary Clause 6





ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล
เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕

โดยที่เป็นการสมควรกำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ โดยให้เป็นไปตามมาตรฐานขั้นต่ำที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลประกาศกำหนด เพื่อให้การคุ้มครองข้อมูลส่วนบุคคลในระยะแรกที่กฎหมายมีผลใช้บังคับมีความเหมาะสม

อาศัยอำนาจตามความในมาตรา ๑๖ (๔) และมาตรา ๓๗ (๑) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล จึงออกประกาศไว้ ดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า "ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕"

ข้อ ๒ ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศในราชกิจจานุเบกษาเป็นต้นไป

ข้อ ๓ ในประกาศนี้

"ความมั่นคงปลอดภัย" หมายความว่า การธำรงไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของข้อมูลส่วนบุคคล ทั้งนี้ เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ

ข้อ ๔ ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ โดยมาตรการรักษาความมั่นคงปลอดภัยดังกล่าว อย่างน้อยต้องมีการดำเนินการ ดังต่อไปนี้

(๑) มาตรการรักษาความมั่นคงปลอดภัยดังกล่าว จะต้องครอบคลุมการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล ตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล ไม่ว่าข้อมูลส่วนบุคคลดังกล่าวจะอยู่ในรูปแบบเอกสารหรือในรูปแบบอิเล็กทรอนิกส์ หรือรูปแบบอื่นใดก็ตาม

(๒) มาตรการรักษาความมั่นคงปลอดภัยดังกล่าว จะต้องประกอบด้วยมาตรการเชิงองค์กร (organizational measures) และมาตรการเชิงเทคนิค (technical measures) ที่เหมาะสม ซึ่งอาจรวมถึงมาตรการทางกายภาพ (physical measures) ที่จำเป็นด้วย โดยคำนึงถึงระดับความเสี่ยงตามลักษณะและวัตถุประสงค์ของการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล ตลอดจนโอกาสเกิดและผลกระทบจากเหตุการละเมิดข้อมูลส่วนบุคคล

"ความมั่นคงปลอดภัย" หมายความว่า การธำรงไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของข้อมูลส่วนบุคคล ทั้งนี้ เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจาก อำนาจหรือโดยมิชอบ

(๒) มาตรการรักษาความมั่นคงปลอดภัยดังกล่าว จะต้องประกอบด้วยมาตรการเชิงองค์กร (organizational measures) และมาตรการเชิงเทคนิค (technical measures) ที่เหมาะสม ซึ่งอาจ รวมถึงมาตรการทางกายภาพ (physical measures) ที่จำเป็นด้วย โดยคำนึงถึงระดับความเสี่ยงตามลักษณะและวัตถุประสงค์ของการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล ตลอดจนโอกาสเกิด และผลกระทบจากเหตุการละเมิดข้อมูลส่วนบุคคล

Clause 7: Additional ISO 27002 guidance for PII controllers

Clause 7.2.2 Identify lawful basis

Article 6 of the GDPR

— consent from PII principals;

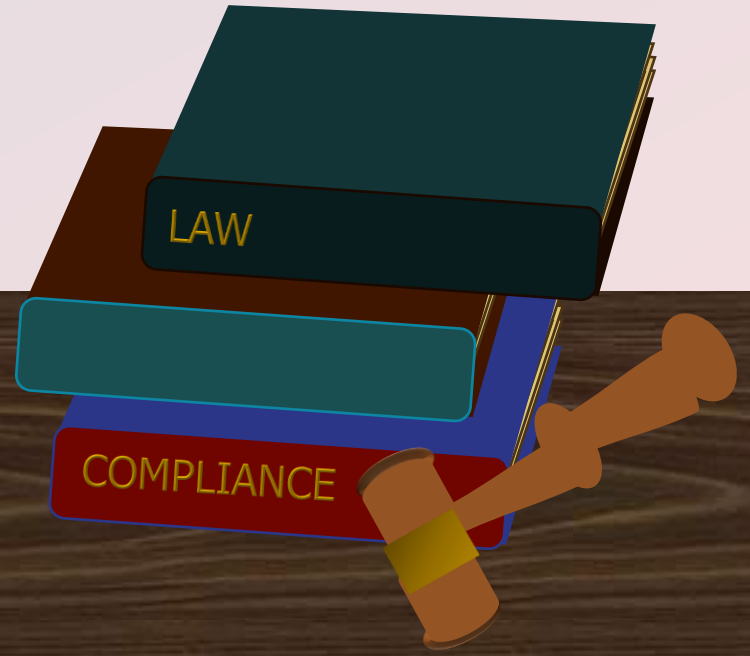
— performance of a contract;

— compliance with a legal obligation;

— protection of the vital interests of PII principals;

— performance of a task carried out in the public interest;

— legitimate interests of the PII controller.



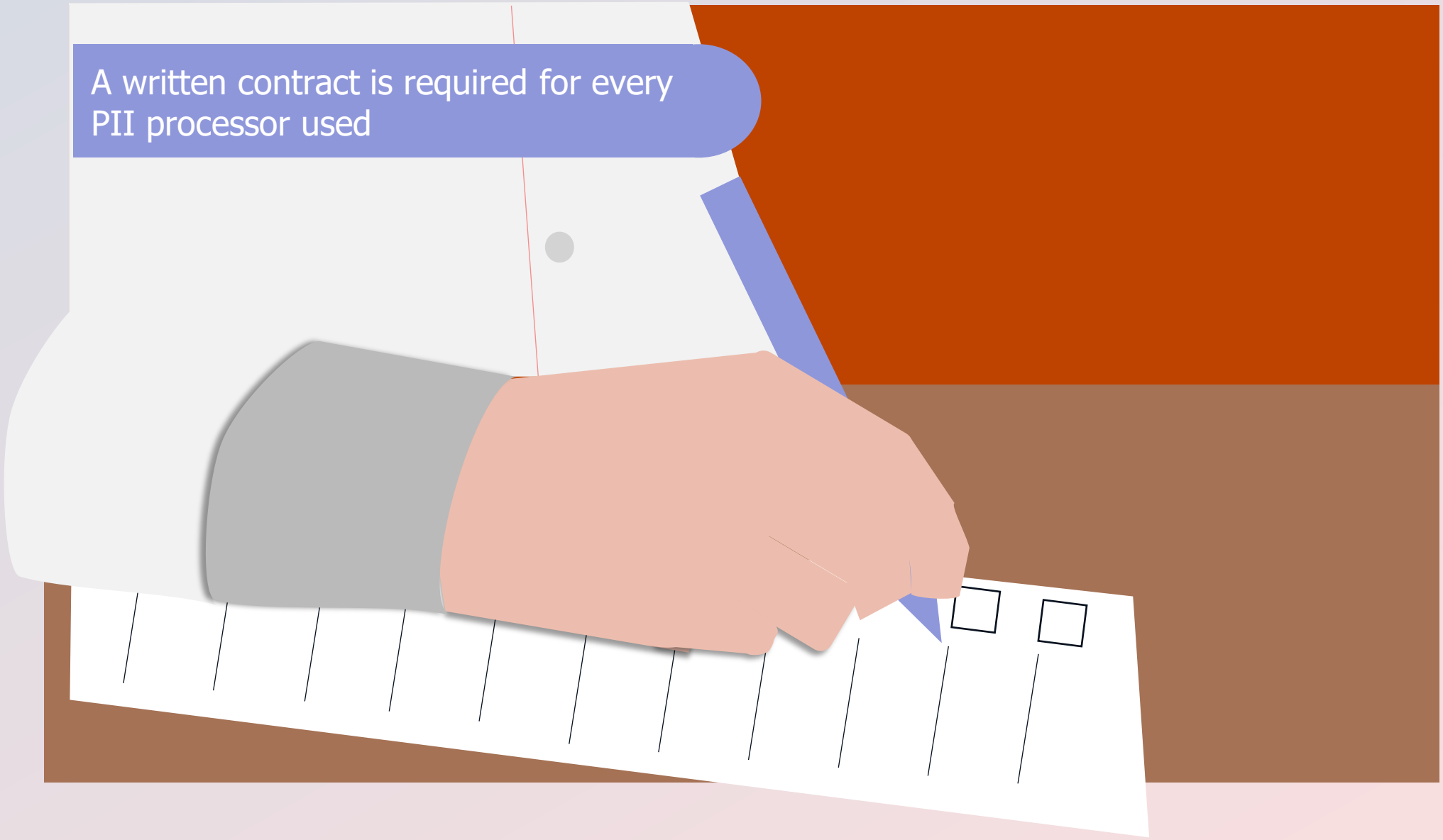
Clause 7.2.3 and Clause 7.2.4

7.2.3 Determine when and how consent is to be obtained

7.2.4 Obtain and record consent

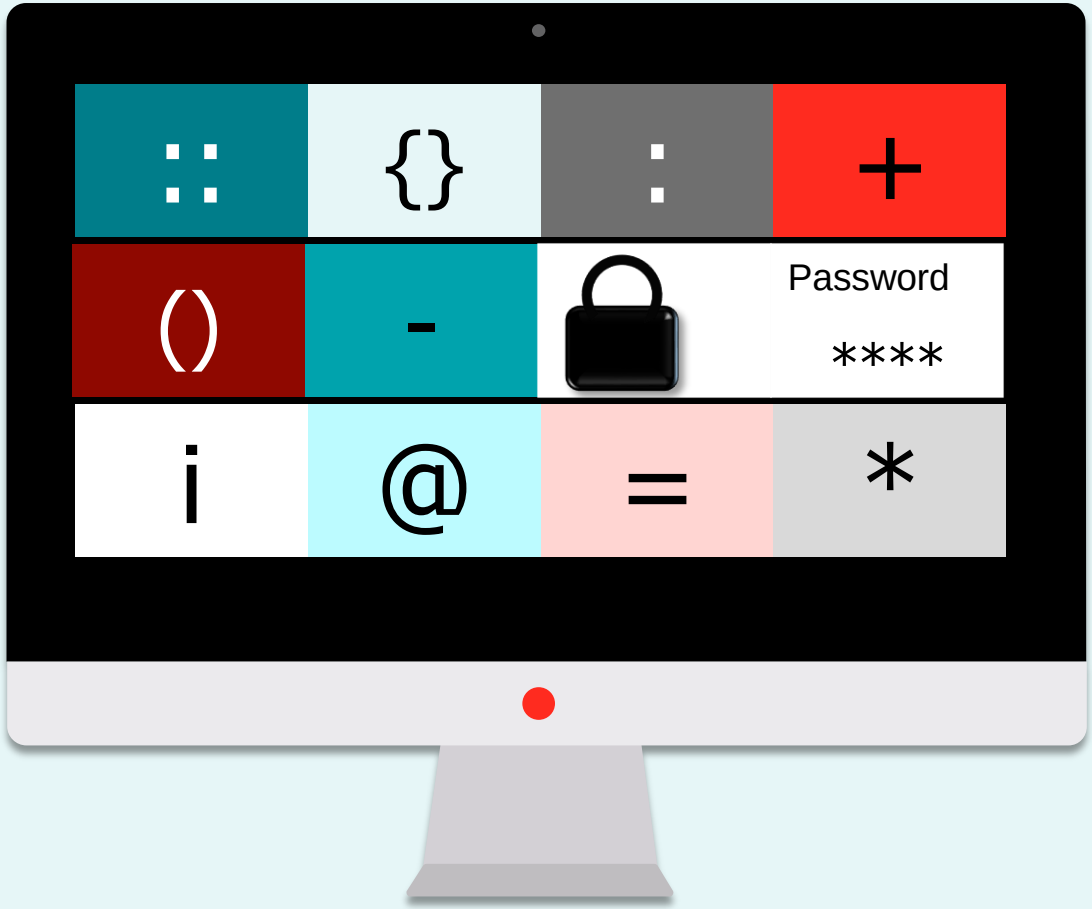
Clause 7.2.5 Privacy impact assessment

Clause 7.2.6 Contracts with PII processors



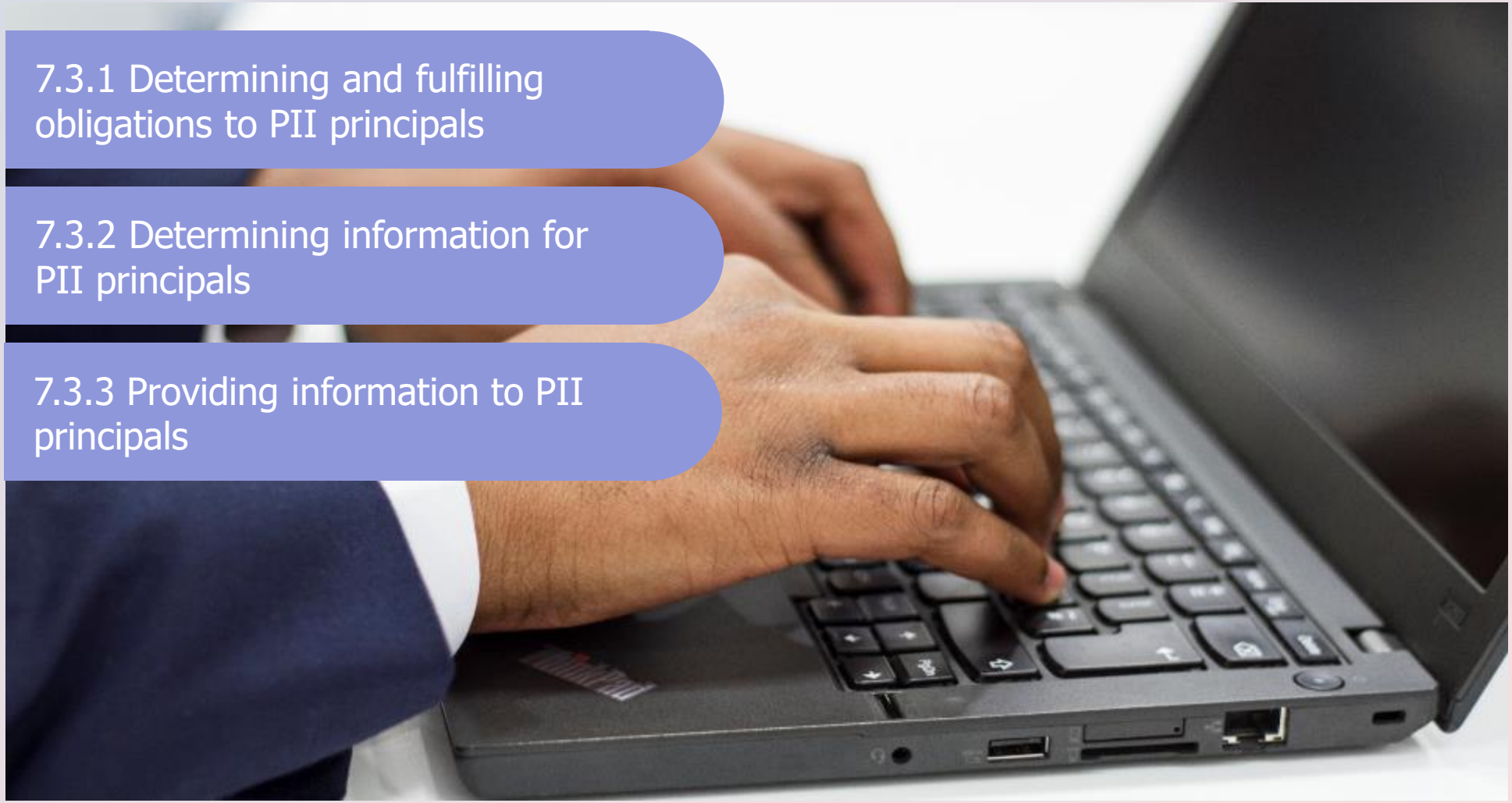
Clause 7.2.7 Joint PII controller

Clause 7.2.8 Records related to processing PII



It is advisable for an organization to have an inventory of processing activities that it undertakes

Clause 7.3.1, Clause 7.3.2 and Clause 7.3.3



Clause 7.3.4, Clause 7.3.5 and Clause 7.3.6

7.3.4 Provide mechanism to modify or withdraw consent

7.3.5 Provide mechanism to object to PII processing

7.3.6 Access, correction and/or erasure

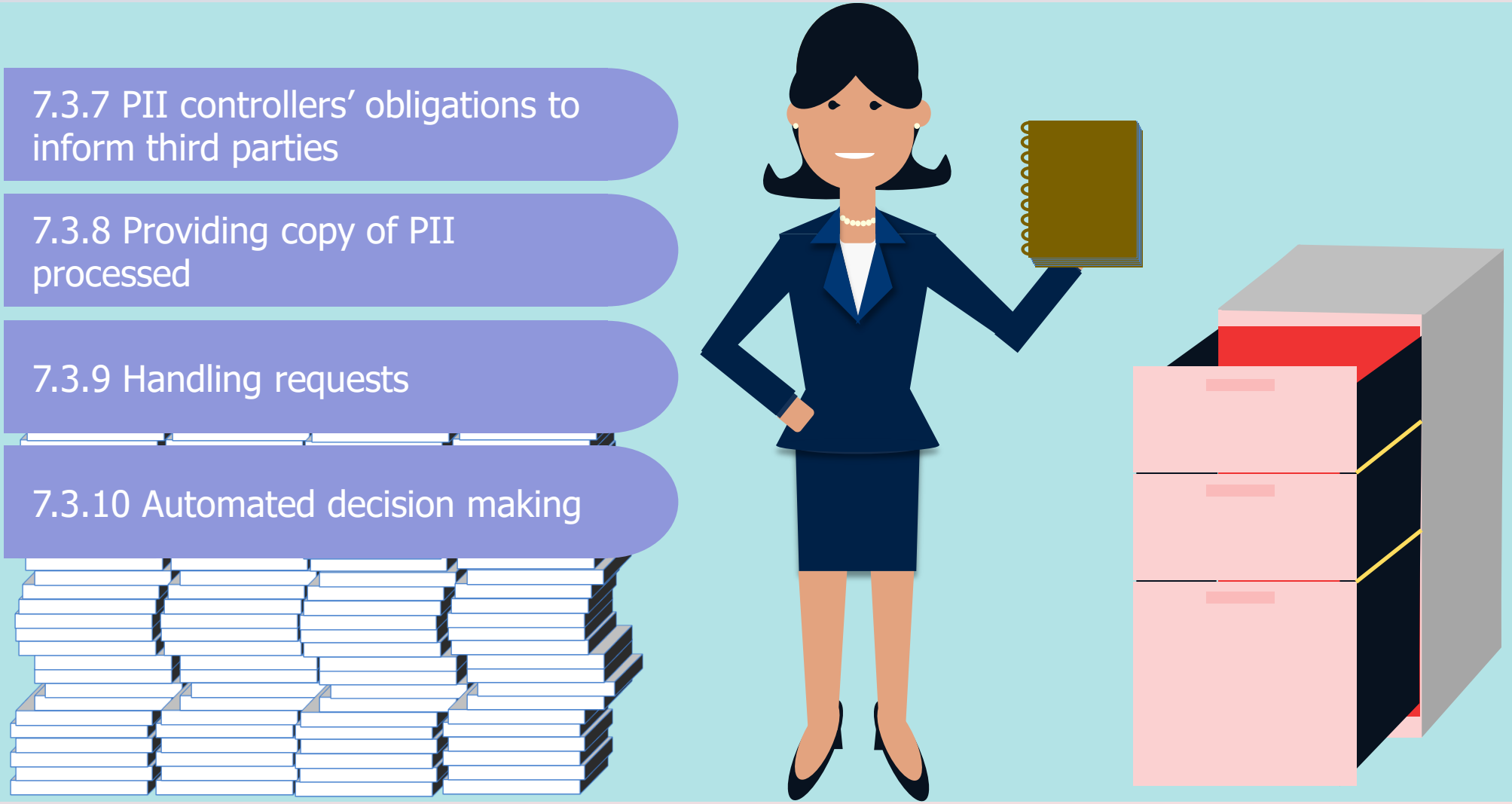
Clause 7.3.7, Clause 7.3.8, Clause 7.3.9 and Clause 7.3.10

7.3.7 PII controllers' obligations to inform third parties

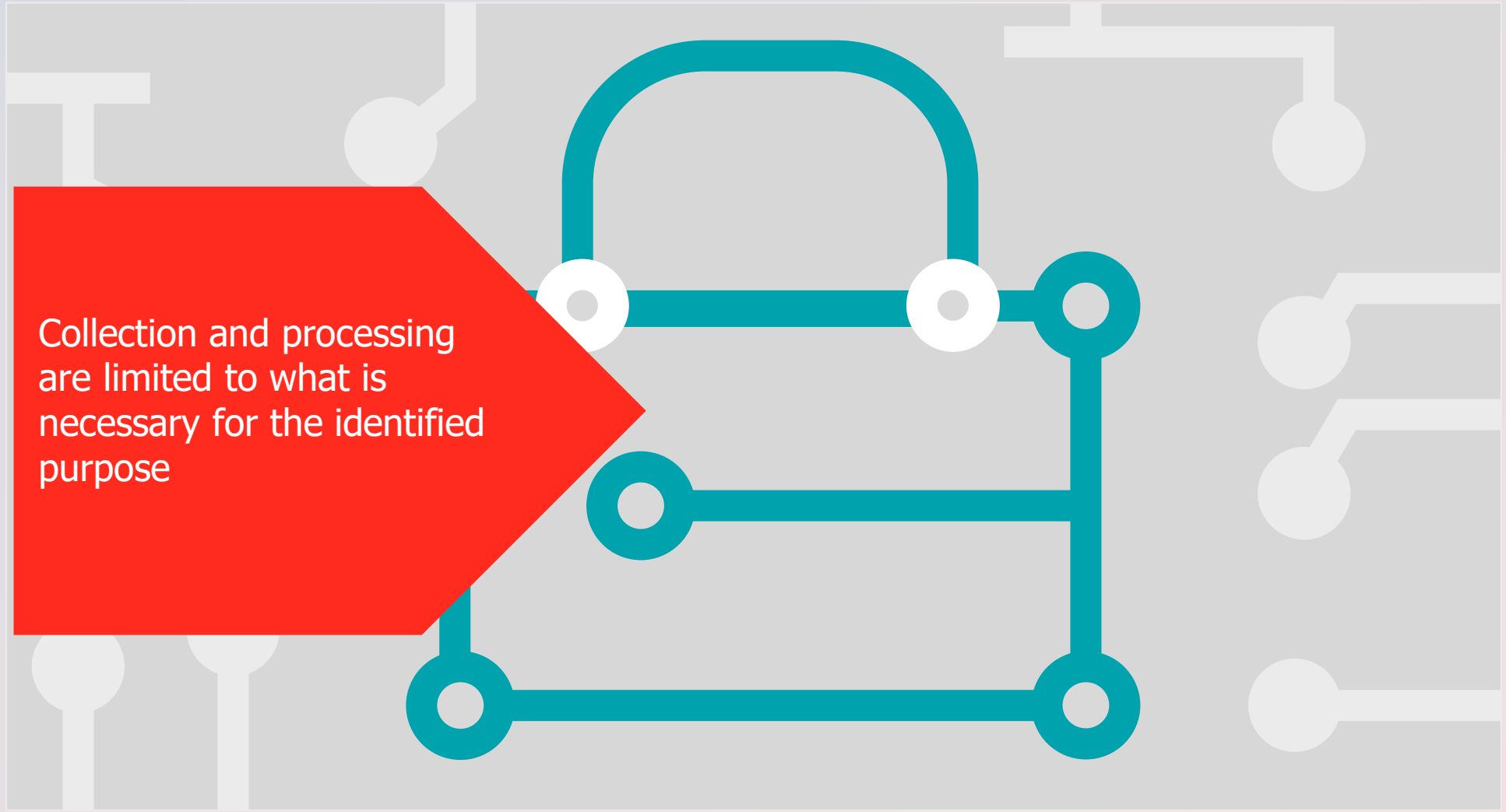
7.3.8 Providing copy of PII processed

7.3.9 Handling requests

7.3.10 Automated decision making



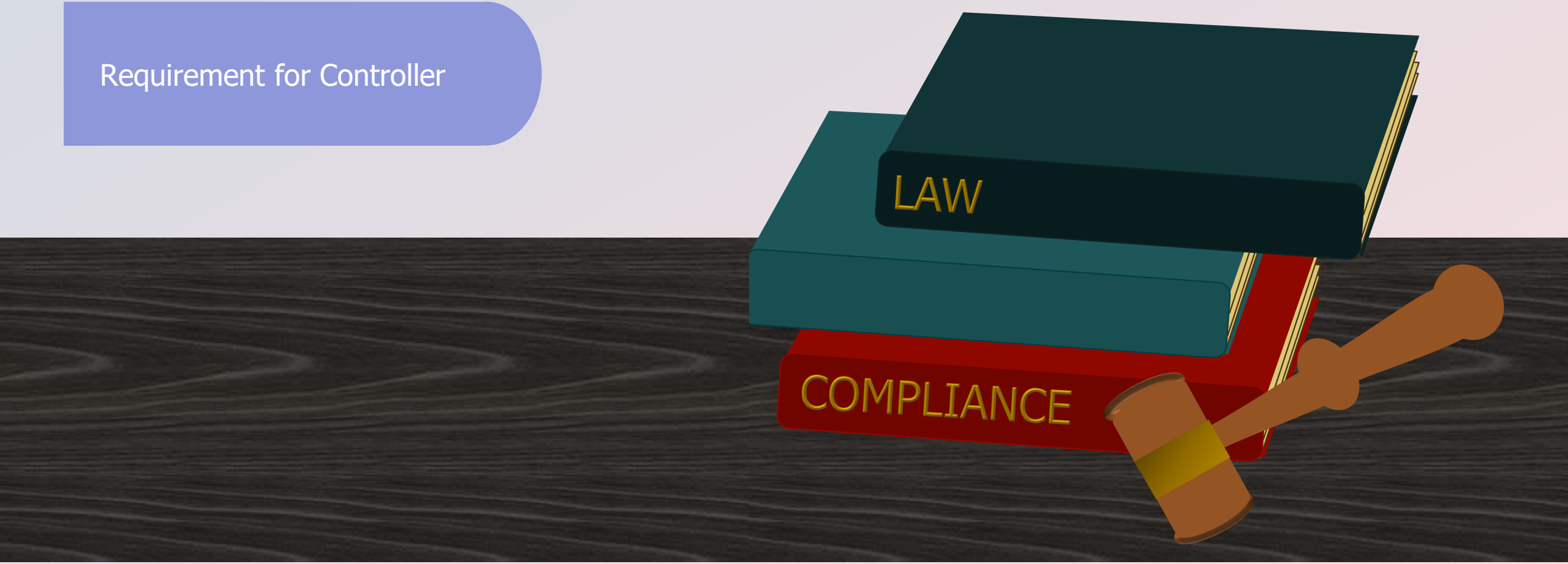
Clause 7.4 Privacy by design and privacy by default



Clause 7.5 PII sharing, transfer and disclosure

Summary Clause 7

Requirement for Controller



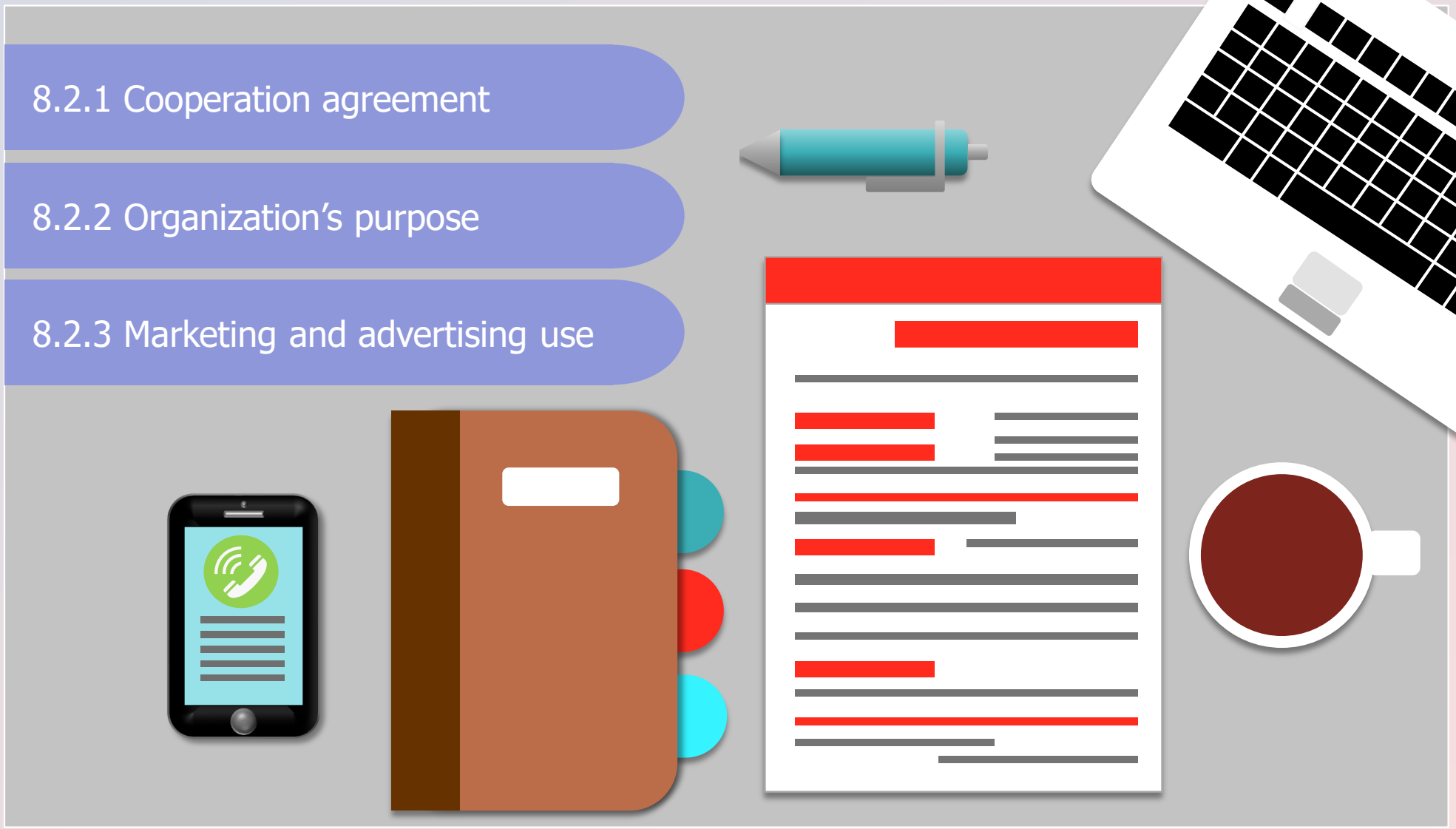
Clause 8: Additional ISO 27002 guidance for PII processors

Clause 8.1, Clause 8.2.2 and Clause 8.2.3

8.2.1 Cooperation agreement

8.2.2 Organization's purpose

8.2.3 Marketing and advertising use



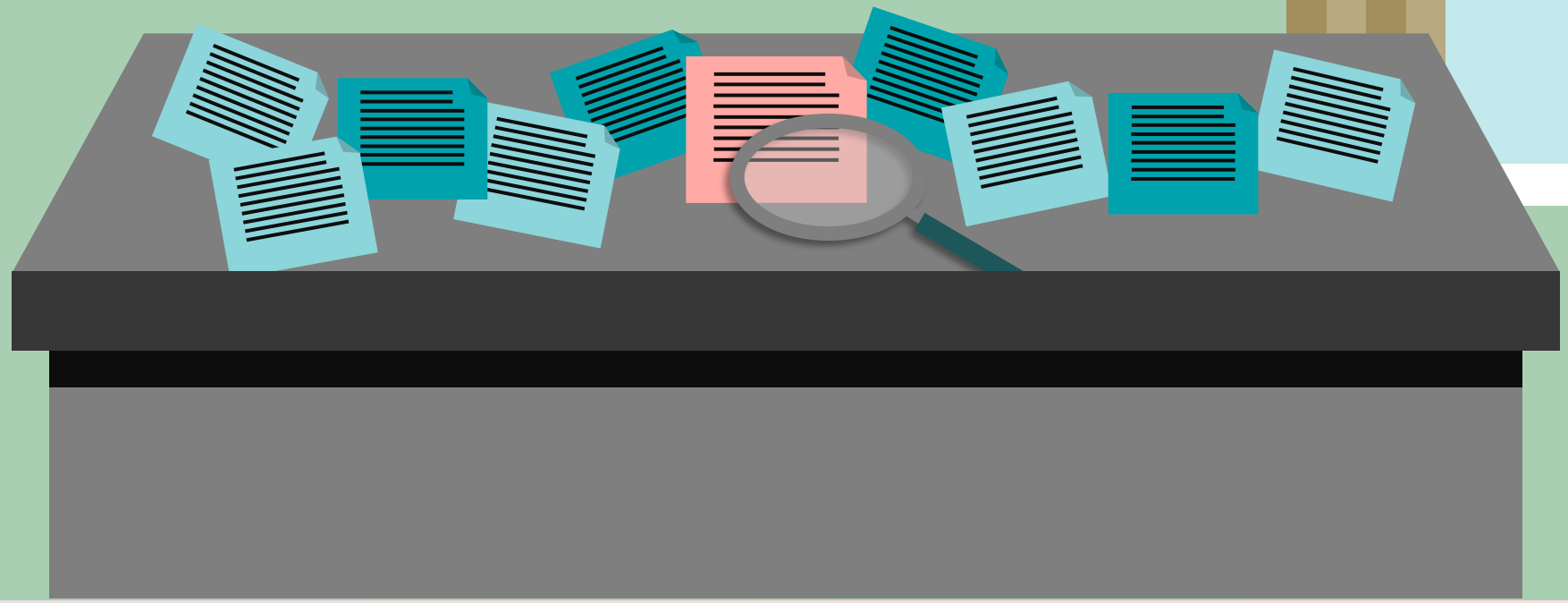
Clause 8.2.4, Clause 8.2.5 and Clause 8.2.6

8.2.4 Infringing instruction

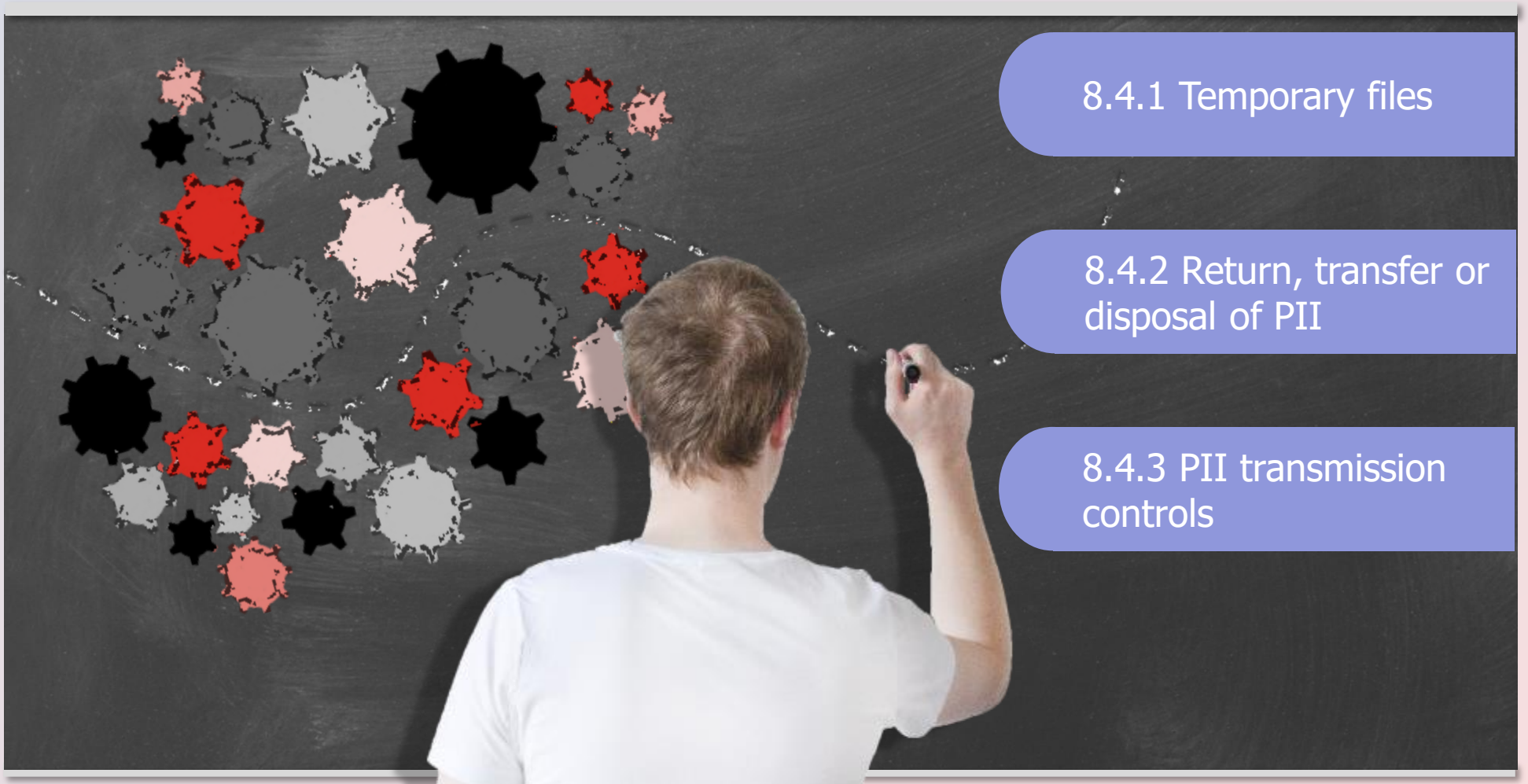
8.2.5 Customer obligations

8.2.6 Records related to processing PII

Clause 8.3.1 Obligations to PII principals



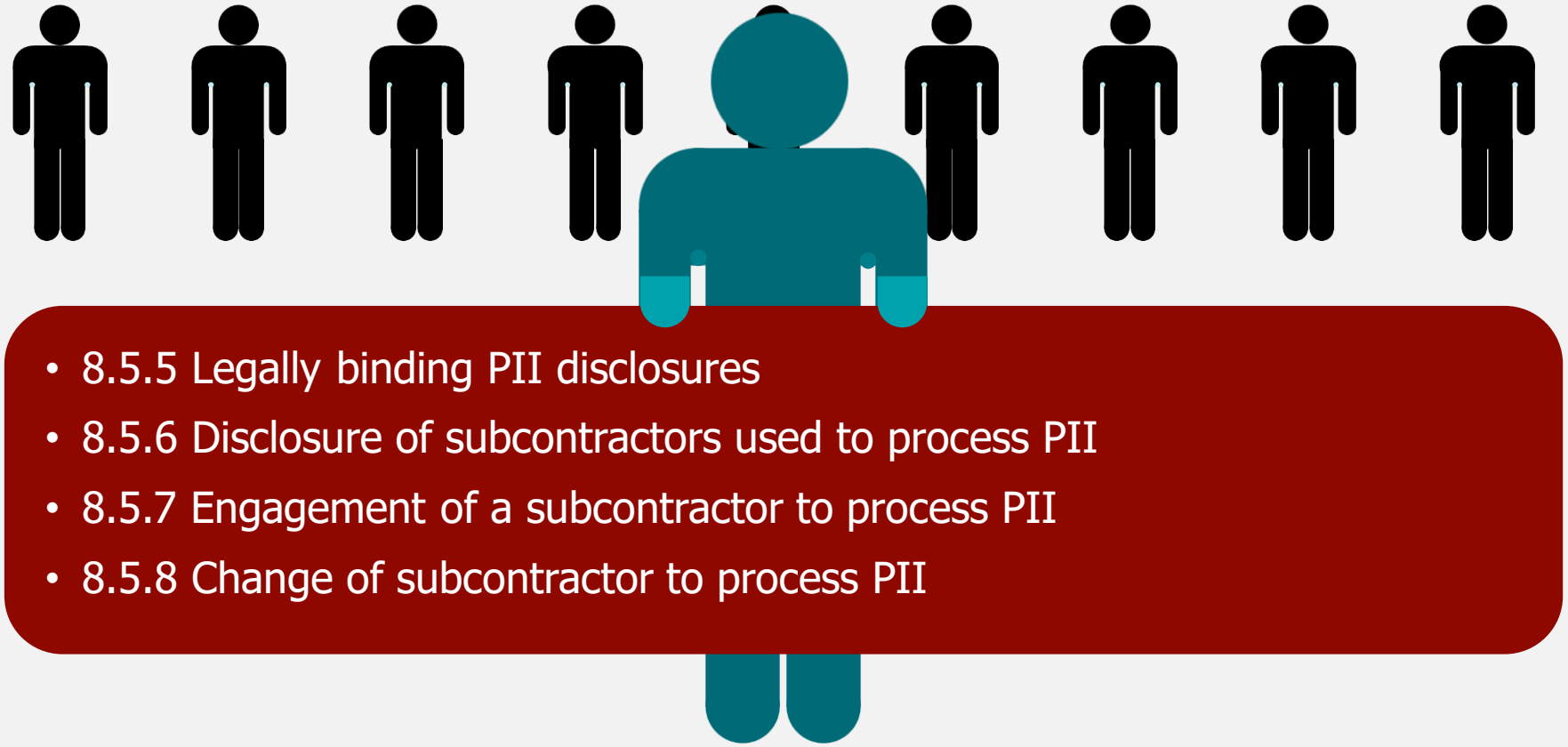
Clause 8.4.1, Clause 8.4.2 and Clause 8.4.3



Clauses 8.5.1 – 8.5.4

- 8.5.1 Basis for PII transfer between jurisdictions
- 8.5.2 Countries and international organizations to which PII might be transferred
- 8.5.3 Records of PII disclosure to third parties
- 8.5.4 Notification of PII disclosure requests

Clauses 8.5.5 – 8.5.8



- 8.5.5 Legally binding PII disclosures
- 8.5.6 Disclosure of subcontractors used to process PII
- 8.5.7 Engagement of a subcontractor to process PII
- 8.5.8 Change of subcontractor to process PII

Summary Clause 8

Requirement for Processor

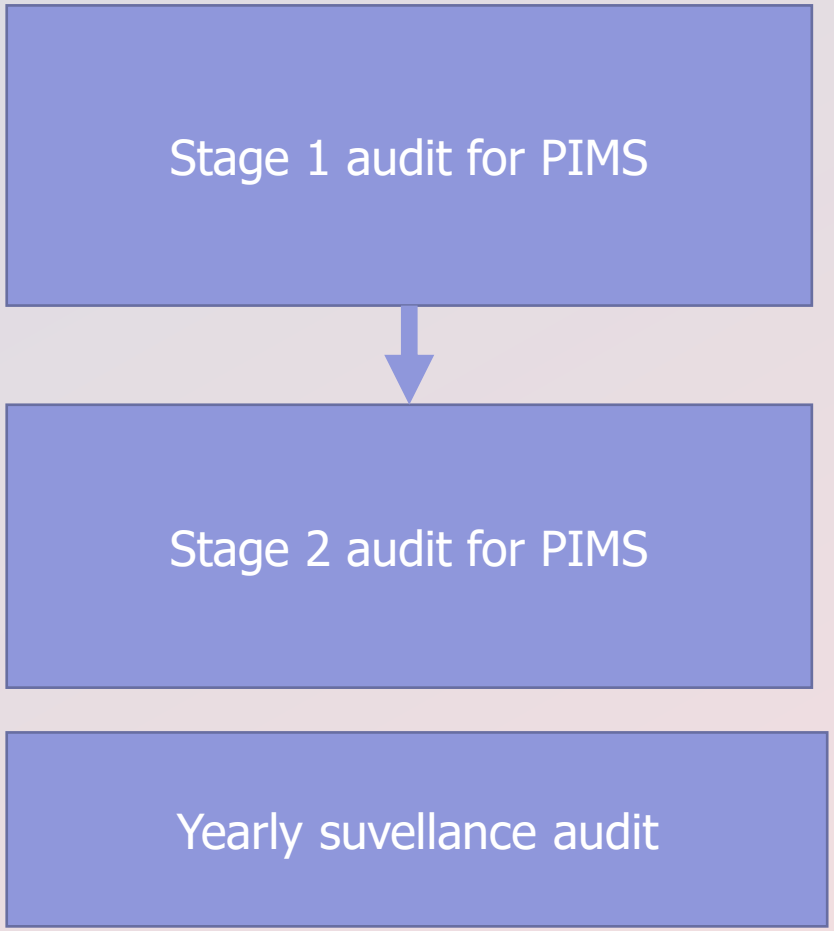
Certify ISO/IEC 27701:2019

Certify ISO/IEC 27701:2019

There is ISMS accredited certificate

Scope of ISMS certificate is covered scope of PIMS

Certify ISO/IEC 27701:2019



Note: Certificate มีอายุ 3 ปี ~~แต่ไม่เกินวันหมดอายุของ ISMS Certificate~~

bsi.

Certification accredit to ANAB

bsi.

Certificate of Registration

PRIVACY INFORMATION MANAGEMENT SYSTEM - ISO/IEC 27701:2019

This is to certify that:

Bangkok
10120
Thailand

Holds Certificate Number: **PM**

and operates a Privacy Information Management System which complies with the requirements of ISO/IEC 27701:2019 for the following scope:

For and on behalf of BSI:

Chris Cheung, Head of Compliance & Risk - Asia Pacific

Original Registration Date: xxxxx
Latest Revision Date: xxxxx

Effective Date: xxxxx
Expiry Date: xxxxx

Page: 1 of 1

...making excellence a habit.™

bsi.

Certificate of Registration

INFORMATION SECURITY MANAGEMENT SYSTEM - ISO/IEC 27001:2013

This is to certify that:

Bangkok
10120
Thailand

Holds Certificate Number: **IS**

and operates an Information Security Management System which complies with the requirements of ISO/IEC 27001:2013 for the following scope:

For and on behalf of BSI:

Chris Cheung, Head of Compliance & Risk - Asia Pacific

Original Registration Date: xxxxx
Latest Revision Date: xxxxx

Effective Date: xxxxx
Expiry Date: xxxxx

Page: 1 of 1

...making excellence a habit.™

This certificate was issued electronically and remains the property of BSI and is bound by the conditions of contract.
An electronic certificate can be authenticated
Printed copies can be validated at www.bsi-global.com/ClientDirectory or telephone +66(2) 2944889-92.
Further clarifications regarding the scope of this certificate and the applicability of ISO/IEC 27001:2013 requirements may be obtained by consulting the organization. This certificate is valid only if provided original copies are in complete set.

Information and Contact: BSI, Kitemark Court, Davy Avenue, Knowlhill, Milton Keynes MK5 8PP. Tel: + 44 345 080 9000
BSI Assurance UK Limited, registered in England under number 7805321 at 389 Chiswick High Road, London W4 4AL, UK.
A Member of the BSI Group of Companies.

bsi.

ผลกระทบของการปรับเปลี่ยน ISO/IEC 27001:2022

New Chapter of ISO/IEC 27001:2022 and ISO/IEC 27002:2022

February 2022

October 2022

bsi.

การเปลี่ยนแปลง ISO/IEC 27002 ต่อ ISO/IEC 27001

ISO/IEC 27001
Information Security Management System requirement

For the assessment and treatment of information security risks tailored to the needs of the organization

Information Security Control Annex A (A5-A18)

ISO/IEC 27002
Code of practice for information security controls

Information Security control
Practice
Requirement 5 – 18

Changed

ISO/IEC 27002

Information security, cybersecurity and privacy protection — Information security controls

Version 2022

Changed in Security control

การเปลี่ยนแปลง ISO/IEC 27001:2022 ต่อ ISO/IEC 27701:2019

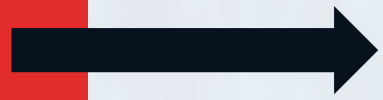
ISO/IEC 27701:2019

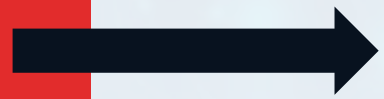
Clause 5: PIMS-specific requirements related to ISO/IEC 27001

Clause 6: PIMS-specific guidance related to ISO/IEC 27002

Clause 7: Additional ISO/IEC 27002 guidance for PII controllers

Clause 8: Additional ISO/IEC 27002 guidance for PII processors





มีผลกระทบ

มีผลกระทบ

การเปลี่ยนแปลง ISO/IEC 27001:2022 ต่อ ISO/IEC 27701:2019

Clause 5: PIMS-specific requirements related to ISO/IEC 27001	→	**Implement as ISO/IEC 27001:2022 Cl. 4-10**

ISO/IEC 27001:2022 Annex A

Clause 5	Organizational controls 37 controls, 34 existing, 3 new
Clause 7	Physical controls 14 controls, 13 existing, 1 new
Clause 6	People controls 8 controls, all existing
Clause 8	Technological controls 34 controls, 27 existing, 7 new

การเปลี่ยนแปลง ISO/IEC 27001:2022 ต่อ ISO/IEC 27701:2019

Clause 6: PIMS-specific guidance related to ISO/IEC 27002

Correspondence of ISO/IEC 27001:2022 (Annex A) with ISO/IEC 27001:2013 (Annex A)		
Correspondence between controls in ISO/IEC 27001:2022 (Annex A) and controls in ISO/IEC 27001:2013 (Annex A)		
ISO/IEC 27001:2022 (Annex A)	**ISO/IEC 27001:2013 (Annex A)**	**Control name according to ISO/IEC 27001:2022 (Annex A)**
5.1	A.5.1.1, A.5.1.2	Policies for information security
5.2	A.6.1.1	Information security roles and responsibilities
5.3	A.6.1.2	Segregation of duties
5.4	A.7.2.1	Management responsibilities
5.5	A.6.1.3	Contact with authorities
5.6	A.6.1.4	Contact with special interest groups
5.7	New	Threat intelligence
5.8	A.6.1.5, A.14.1.1	Information security in project management
5.9	A.8.1.1, A.8.1.2	Inventory of information and other associated assets
5.10	A.8.1.3, A.8.2.3	Acceptable use of information and other associated assets
5.11	A.8.1.4	Return of assets
5.12	A.8.2.1	Classification of information
5.13	A.8.2.2	Labelling of information
5.14	A.13.2.1, A.13.2.2, A.13.2.3	Information transfer
5.15	A.9.1.1, A.9.1.2	Access control

• Contact us

www.bsigroup.com/th-TH/

BSI Thailand

@bsithailand

Tel: 02 294 4889-92 Email: infothai@bsigroup.com