



Your partner
in progress

มีอะไรเปลี่ยนแปลงใน *ISO/IEC 27701* *New version*

(Draft for public comment 02 July 2024)

บรรยายโดย

อาจารย์กิตติพงษ์ เกียรตินิยมรุ่ง

Product Technical Manager, BSI Thailand



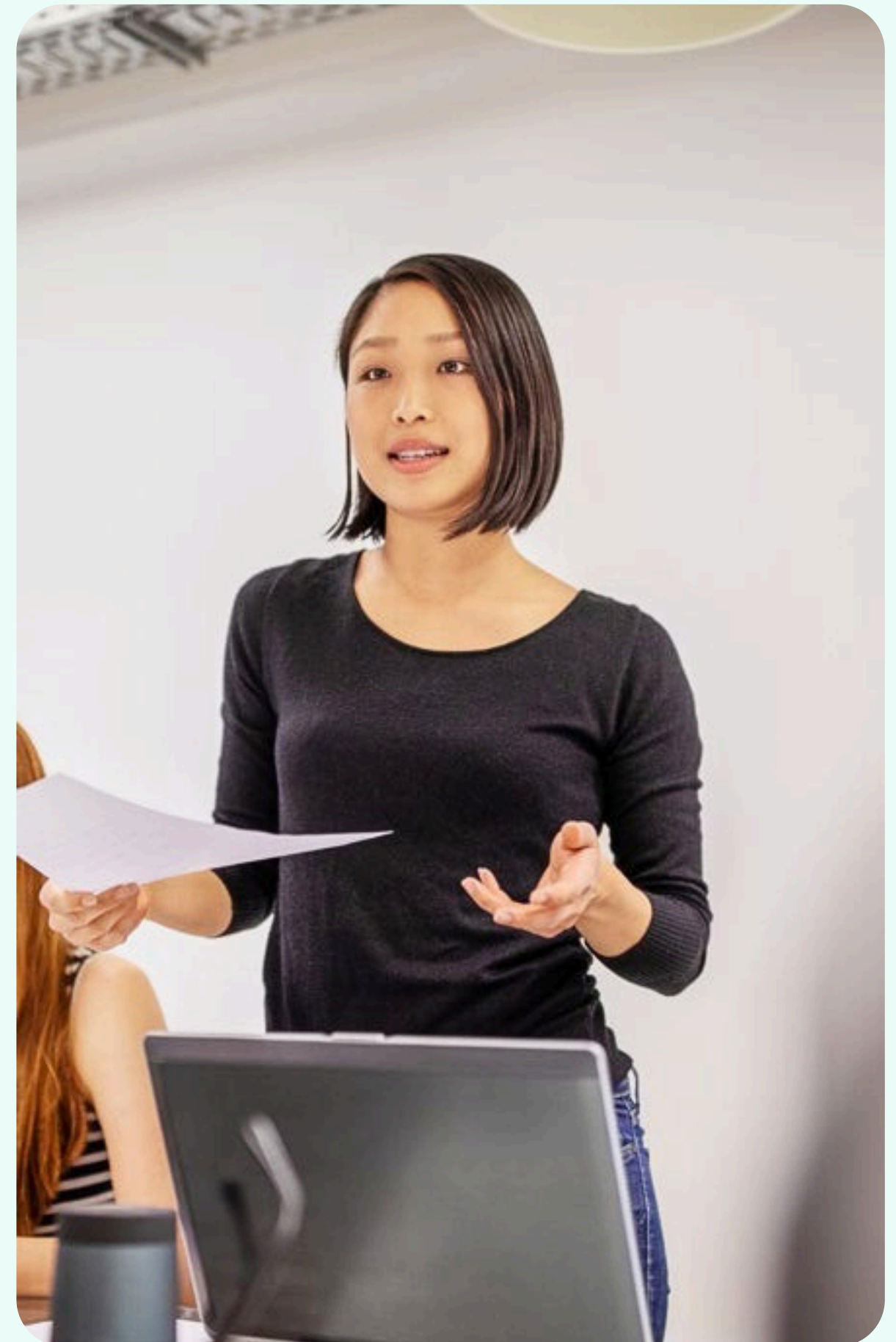
หัวข้อชวนคุย

1

ข้อกำหนด ISO/IEC 27701
New version (Draft for
public comment
02 July 2024)

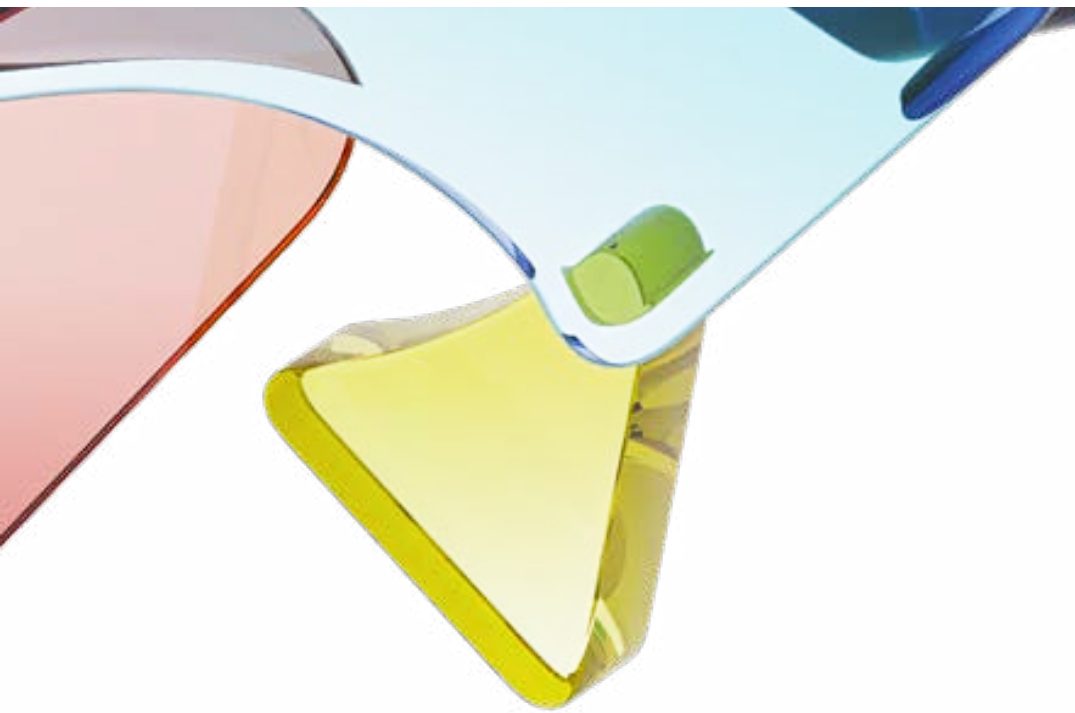
2

แนวทางการปรับเปลี่ยนผ่าน
ไปสู่ ISO/IEC 27001
New version
(Draft for public
comment 02 July 2024)



ข้อกำหนด *ISO/IEC 27701*
New version
(ISO/IEC DIS 27701.2
Vote terminate
on: 2024-08-27)






- ISO/IEC DIS 27701.2
Vote terminate on : 2024-08-27

Information security, cybersecurity and privacy protection – Privacy information management system – Requirement and guidance



	<p>DRAFT International Standard</p> <p>ISO/IEC DIS 27701.2</p>
<p>Information security, cybersecurity and privacy protection — Privacy information management systems — Requirements and guidance</p> <p>ICS: 35.030</p>	<p>ISO/IEC JTC 1/SC 27 Secretariat: DIN Voting begins on: 2024-07-02 Voting terminates on: 2024-08-27</p>
<p>This document is circulated as received from the committee secretariat.</p> <p>ISO/CEN PARALLEL PROCESSING</p> <p>IMPORTANT — Please use this updated version dated 2024-06-19, and discard any previous version of this DIS as VA relation has been added.</p> <p>Reference number ISO/IEC DIS 27701.2:2024(en)</p>	<p><small>THIS DOCUMENT IS A DRAFT CIRCULATED FOR COMMENTS AND APPROVAL. IT IS THEREFORE SUBJECT TO CHANGE AND MAY NOT BE REFERRED TO AS AN INTERNATIONAL STANDARD UNTIL PUBLISHED AS SUCH.</small></p> <p><small>IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.</small></p> <p><small>REPRINTS OF THIS DRAFT ARE INVITED TO SUBMIT WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.</small></p> <p>© ISO/IEC 2024</p>



- ISO/IEC DIS 27701.2
Vote terminate on : 2024-08-27

Information security,
cybersecurity and privacy
protection – Privacy
information management
system – Requirement and
guidance



Contents	Page
Foreword.....	viii
Introduction.....	ix
1 Scope	1
2 Normative references	1
3 Terms, definitions and abbreviations	1
4 Context of the organization.....	5
4.1 Understanding the organization and its context.....	5
4.2 Understanding the needs and expectations of interested parties.....	5
4.3 Determining the scope of the privacy information management system.....	6
4.4 Privacy information management system.....	6
5 Leadership.....	7
5.1 Leadership and commitment	7
5.2 Privacy Policy.....	7
5.3 Roles, responsibilities and authorities.....	7
6 Planning	8
6.1 Actions to address risks and opportunities	8
6.1.1 General	8
6.1.2 Privacy risk assessment.....	8
6.1.3 Privacy risk treatment.....	9
6.2 Privacy objectives and planning to achieve them.....	10
6.3 Planning of changes	10
7 Support.....	10
7.1 Resources	10
7.2 Competence	10
7.3 Awareness	11
7.4 Communication	11
7.5 Documented information	11
7.5.1 General	11
7.5.2 Creating and updating documented information	11
7.5.3 Control of documented information	12
8 Operation.....	12
8.1 Operational planning and control	12
8.2 Privacy risk assessment.....	12
8.3 Privacy risk treatment.....	13
9 Performance evaluation.....	13
9.1 Monitoring, measurement, analysis and evaluation	13
9.2 Internal audit.....	13
9.2.1 General	13
9.2.2 Internal audit programme	13
9.3 Management review	14
9.3.1 General	14
9.3.2 Management review inputs.....	14



- ISO/IEC DIS 27701.2
Vote terminate on : 2024-08-27

Information security,
cybersecurity and privacy
protection – Privacy
information management
system – Requirement and
guidance

9.3.3	Management review results	14
10	Improvement	14
10.1	Continual improvement	14
10.2	Nonconformity and corrective action	14
11	Further information on Annexes	15
Annex A (normative)	PIMS reference control objectives and controls for PII Controllers and PII Processors	16
Annex B (normative)	Implementation guidance for PII Controllers and PII processors	23
B.1	Implementation guidance for PII controllers	23
B.1.1	General	23
B.1.2	Conditions for collection and processing	23
B.1.2.1	Objective	23
B.1.2.2	Identify and document purpose	23
B.1.2.3	Identify lawful basis	23
B.1.2.4	Determine when and how consent is to be obtained	24
B.1.2.5	Obtain and record consent	24
B.1.2.6	Privacy impact assessment	25
B.1.2.7	Contracts with PII processors	25
B.1.2.8	Joint PII controller	26
B.1.2.9	Records related to processing PII	26
B.1.3	Obligations to PII principals	27
B.1.3.1	Objective	27
B.1.3.2	Determining and fulfilling obligations to PII principals	27
B.1.3.3	Determining information for PII principals	27
B.1.3.4	Providing information to PII principals	28
B.1.3.5	Providing mechanism to modify or withdraw consent	28
B.1.3.6	Providing mechanism to object to PII processing	29
B.1.3.7	Access, correction or erasure	29
B.1.3.8	PII controllers' obligations to inform third parties	30
B.1.3.9	Providing copy of PII processed	30
B.1.3.10	Handling requests	30
B.1.3.11	Automated decision making	31
B.1.4	Privacy by design and privacy by default	31
B.1.4.1	Objective	31
B.1.4.2	Limit collection	31
B.1.4.3	Limit processing	31
B.1.4.4	Accuracy and quality	32



- ISO/IEC DIS 27701.2
Vote terminate on : 2024-08-27

Information security,
cybersecurity and privacy
protection – Privacy
information management
system – Requirement and
guidance



B.1.4.5 PII minimization objectives	32
B.1.4.6 PII de-identification and deletion at the end of processing	33
B.1.4.7 Temporary files	33
B.1.4.8 Retention	33
B.1.4.9 Disposal	34
B.1.4.10 PII transmission controls.....	34
B.1.5 PII sharing, transfer and disclosure.....	34
B.1.5.1 Objective	34
B.1.5.2 Identify basis for PII transfer between jurisdictions.....	34
B.1.5.3 Countries and international organizations to which PII can be transferred	35
B.1.5.4 Records of transfer of PII.....	35
B.1.5.5 Records of PII disclosure to third parties	35
B.2 Implementation guidance for PII processors	35
B.2.1 General	35
B.2.2 Conditions for collection and processing.....	36
B.2.2.1 Objective	36
B.2.2.2 Customer agreement	36
B.2.2.3 Organization's purposes	36
B.2.2.4 Marketing and advertising use	37
B.2.2.5 Infringing instruction.....	37
B.2.2.6 Customer obligations	37
B.2.2.7 Records related to processing PII.....	37
B.2.3 Obligations to PII principals	37
B.2.3.1 Objective	38
B.2.3.2 Comply with obligations to PII principals	38
B.2.4 Privacy by design and privacy by default	38
B.2.4.1 Objective	38
B.2.4.2 Temporary files	38
B.2.4.3 Return, transfer or disposal of PII.....	38
B.2.4.4 PII transmission controls.....	39
B.2.5 PII sharing, transfer and disclosure.....	39
B.2.5.1 Objective	39
B.2.5.2 Basis for PII transfer between jurisdictions	39
B.2.5.3 Countries and international organizations to which PII can be transferred	40
B.2.5.4 Records of PII disclosures to third parties	40
B.2.5.5 Notification of PII disclosure requests.....	40



- ISO/IEC DIS 27701.2
Vote terminate on : 2024-08-27

Information security,
cybersecurity and privacy
protection – Privacy
information management
system – Requirement and
guidance



B.2.5.6 Legally binding PII disclosures	41
B.2.5.7 Disclosure of subcontractors used to process PII	41
B.2.5.8 Engagement of a subcontractor to process PII	41
B.2.5.9 Change of subcontractor to process PII.....	42
B.3 Implementation guidance for PII controllers and PII processors	42
B.3.1 Objective.....	42
B.3.2 General.....	42
B.3.3 Policies for information security.....	42
B.3.4 Information security roles and responsibilities	42
B.3.5 Classification of information.....	43
B.3.6 Labelling of information.....	43
B.3.7 Information transfer.....	43
B.3.8 Identity management	44
B.3.9 Access rights.....	44
B.3.10 Addressing information security within supplier agreements	44
B.3.11 Information security incident management planning and preparation.....	45
B.3.12 Response to information security incidents	45
B.3.13 Legal, statutory, regulatory and contractual requirements	47
B.3.14 Protection of records	47
B.3.15 Independent review of information security.....	47
B.3.16 Compliance with policies, rules and standards for information security	48
B.3.17 Information security awareness, education and training	48
B.3.18 Confidentiality or non-disclosure agreements.....	48
B.3.19 Clear desk and clear screen.....	49
B.3.20 Storage media.....	49
B.3.21 Secure disposal or re-use of equipment	49
B.3.22 User endpoint devices	50
B.3.23 Secure authentication.....	50
B.3.24 Information backup	50
B.3.25 Logging.....	51
B.3.26 Use of cryptography	51
B.3.27 Secure development life cycle	52
B.3.28 Application security requirements.....	52
B.3.29 Secure system architecture and engineering principles	52
B.3.30 Outsourced development.....	53
B.3.31 Test information.....	53

- ISO/IEC DIS 27701.2
Vote terminate on : 2024-08-27

Information security, cybersecurity
and privacy protection – Privacy
information management system
Requirement and guidance

Annex C (informative) Mapping to ISO/IEC 29100	54
Annex D (informative) Mapping to the General Data Protection Regulation	57
Annex E (informative) Mapping to ISO/IEC 27018 and ISO/IEC 29151	61
Annex F (informative) Correspondence with ISO/IEC 27701:2019	64
Bibliography	72



ISO/IEC 27701 (Requirement 4-10)



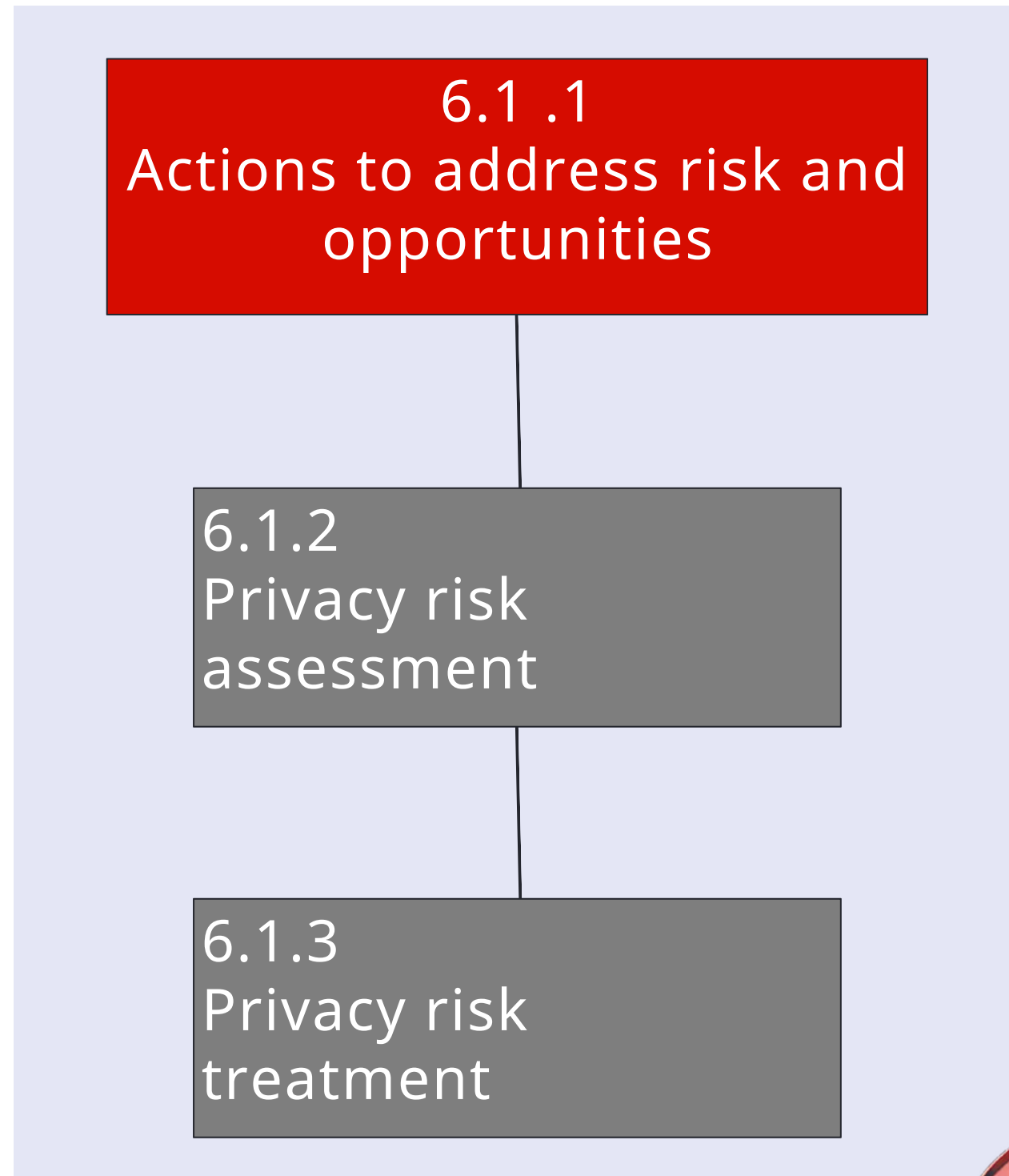
ISO/IEC 27701 (Requirement 4-10) Clause 6.1

6.1.1
Actions to address
risk and
opportunities



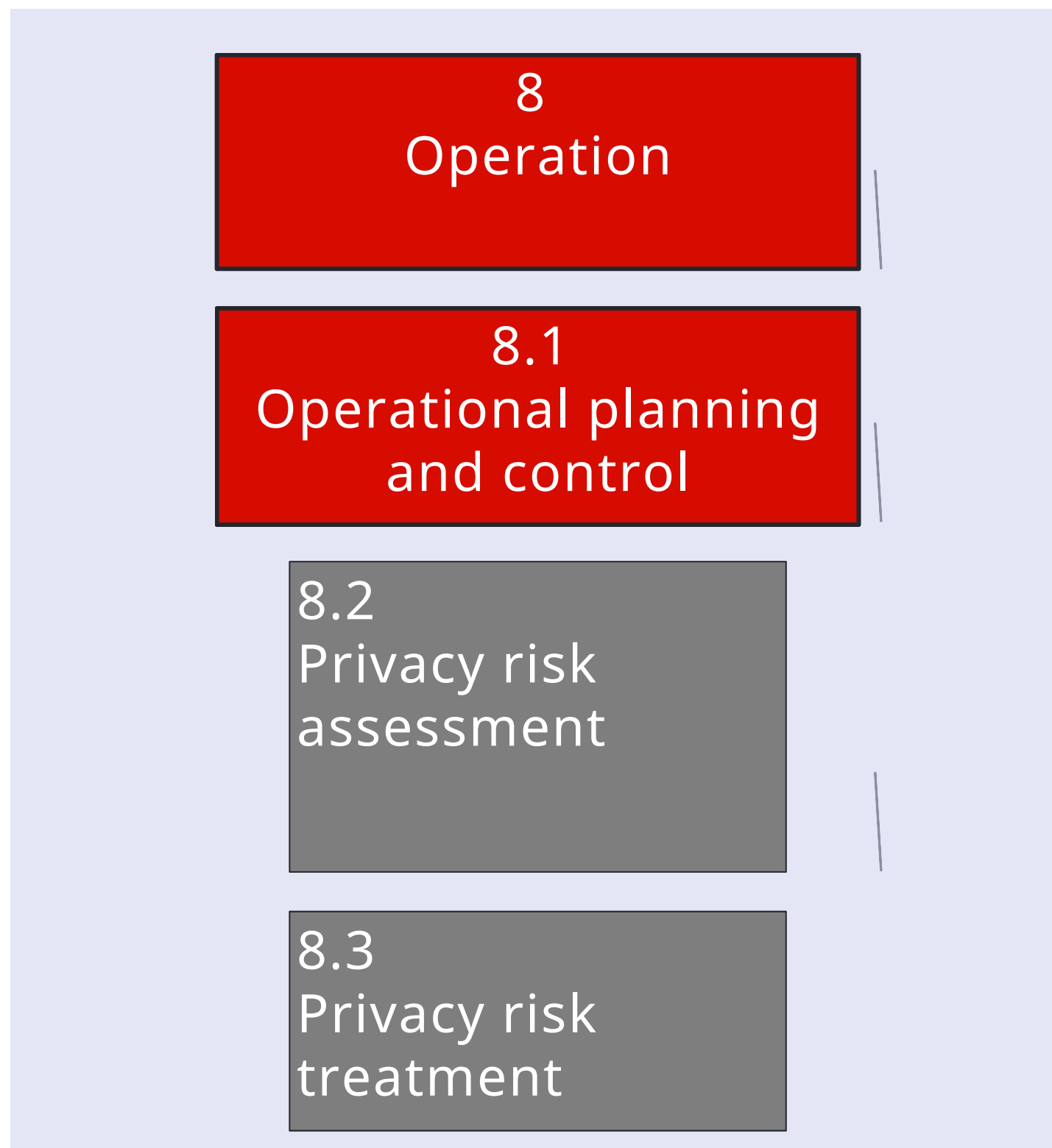
ISO/IEC 27701 (Requirement 4-10)

Clause 6.1



ISO/IEC 27701 (Requirement 4-10)

Clause 8



***Annex A
PIMS Reference
Control Objective
and Control for
PII Controller and
PII Processors***



Example of Annex A

Table A.1 – Control Objective and control for PII controllers

Table A.1 — Control objectives and controls for PII controllers

Conditions for collection and processing		
Objective:		
To determine and document that processing is lawful, with legal basis as per applicable jurisdictions, with clearly defined and legitimate purposes.		
Control reference	Control title	Control
A.1.2.2	Identify and document purpose	The organization shall identify and document the specific purposes for which the PII will be processed.
A.1.2.3	Identify lawful basis	The organization shall determine, document and comply with the relevant lawful basis for the processing of PII for the identified purposes.
A.1.2.4	Determine when and how consent is to be obtained	The organization shall determine and document a process by which it can demonstrate if, when and how consent for the processing of PII was obtained from PII principals.
A.1.2.5	Obtain and record consent	The organization shall obtain and record consent from PII principals according to the documented processes.
A.1.2.6	Privacy impact assessment	The organization shall assess the need for, and implement where appropriate, a privacy impact assessment whenever new processing of PII or changes to existing processing of PII is planned.
A.1.2.7	Contracts with PII processors	The organization shall have a written contract with any PII processor that it uses, and shall ensure that their contracts with PII processors address the implementation of the appropriate controls in Annex A (see Table A.2).
A.1.2.8	Joint PII controller	The organization shall determine respective roles and responsibilities for the processing of PII (including PII protection and security requirements) with any joint PII controller.

A1 – Control Objective and control for PII controllers

Conditions for collection and processing

Objective: To determine and document that processing is lawful, with legal basis as per applicable jurisdictions, and with clearly defined and legitimate purposes.

Control Reference:

A.1.2.2 Identify and document purpose

A.1.2.3 Identify lawful basis

A.1.2.4 Determine when and how consent is to be obtained

A.1.2.5 Obtain and record consent

A.1.2.6 Privacy impact assessment

A.1.2.7 Contracts with PII processors

A.1.2.8 Joint PII controller

A.1.2.9 Records related to processing PII

Obligations to PII principals

Objective: To ensure that PII principals are provided with appropriate information about the processing of their PII and to meet any other applicable obligations to PII principals related to the Processing of their PII.

Control Reference:

A.1.3.2 Determining and fulfilling obligations to PII principals

A.1.3.3 Determining information for PII principals

A.1.3.4 Providing information to PII principals

A.1.3.5 Providing mechanism to modify or withdraw consent

A.1.3.6 Providing mechanism to object to PII processing

A.1.3.7 Access, correction and/or erasure

A.1.3.8 PII controllers' obligations to inform third parties

A.1.3.9 Providing copy of PII processed

A.1.3.10 Handling requests

A.1.3.11 Automated decision making

A1 – Control Objective and control for PII controllers

Privacy by design and privacy by default

Objective: To ensure that processes and systems are designed such that the collection and processing (including use, disclosure, retention, transmission and disposal) are limited to what is necessary for the identified purpose.

Control Reference:

A.1.4.2 Limit collection

A.1.4.3 Limit processing

A.1.4.4 Accuracy and quality

A.1.4.5 PII minimization objectives

A.1.4.6 PII de-identification and deletion at the end of processing

A.1.4.7 Temporary files

A.1.4.8 Retention

A.1.4.8 Disposal

A.1.4.9 PII transmission controls

PII sharing, transfer, and disclosure

Objective: To determine whether and document when PII is shared, transferred to other jurisdictions or third parties and/or disclosed in accordance with applicable obligations.

Control Reference:

A.1.5.2 Identify basis for PII transfer between jurisdictions

A.1.5.3 Countries and international organizations to which PII can be transferred

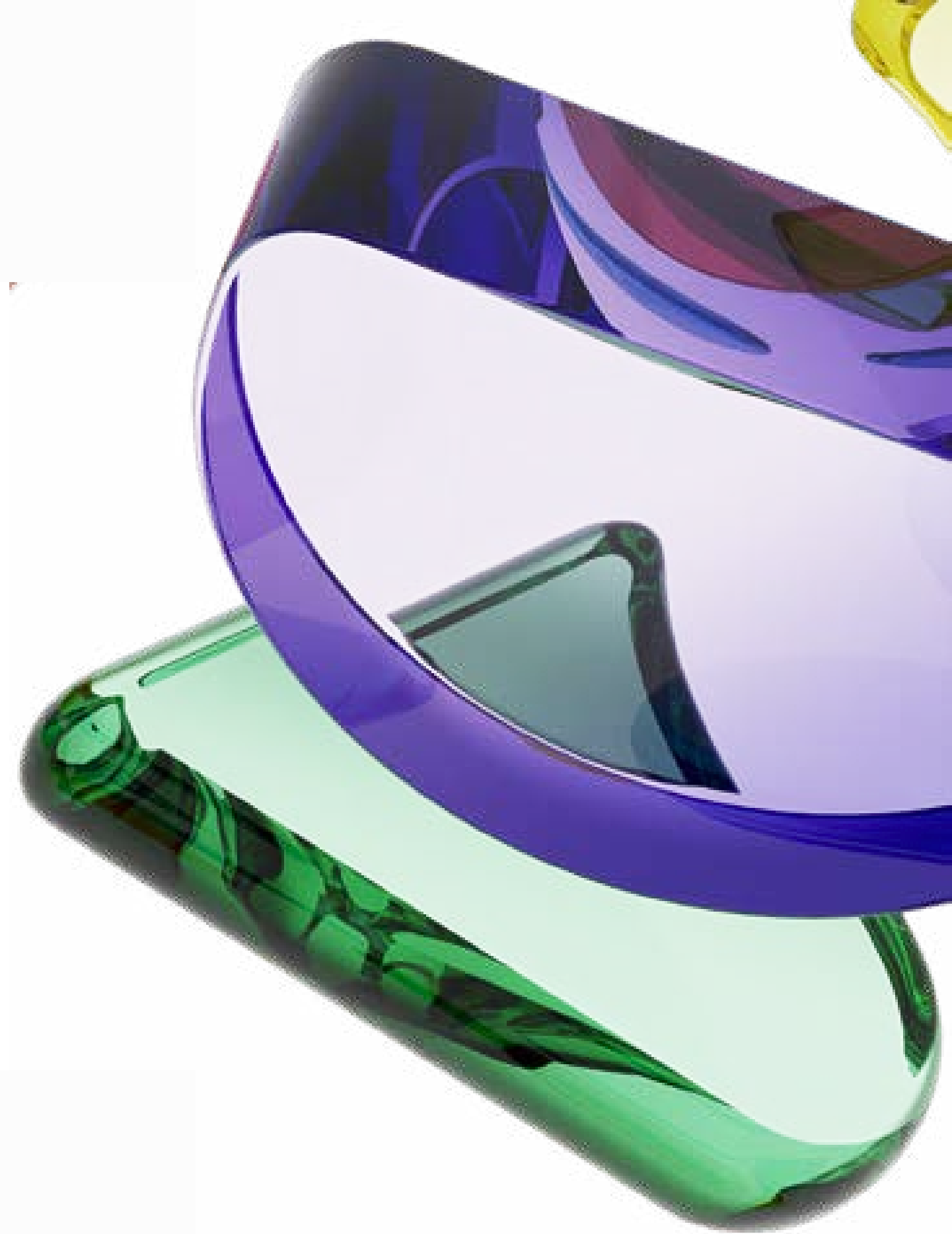
A.1.5.4 Records of transfer of PII

A.1.5.5 Records of PII disclosure to third parties

Example of Annex A

Table A.2 – Control Objective and control for PII processor

Obligations to PII principals		
Objective: To ensure that PII principals are provided with the appropriate information about the processing of their PII, and to meet any other applicable obligations to PII principals related to the processing of their PII.		
A.2.3.2	Comply with obligations to PII principals	The organization shall provide the customer with the means to comply with its obligations related to PII principals.
Privacy by design and privacy by default		
Objective: To ensure that processes and systems are designed such that the collection and processing of PII (including use, disclosure, retention, transmission and disposal) are limited to what is necessary for the identified purpose.		
A.2.4.2	Temporary files	The organization shall ensure that temporary files created as a result of the processing of PII are disposed of (e.g. erased or destroyed) following documented procedures within a specified, documented period.
A.2.4.3	Return, transfer or disposal of PII	The organization shall provide the ability to return, transfer or disposal of PII in a secure manner. It shall also make its policy available to the customer.
A.2.4.4	PII transmission controls	The organization shall subject PII transmitted over a data-transmission network to appropriate controls designed to ensure that the data reaches its intended destination.



A2 – Control Objective and control for PII Processors

Conditions for collection and processing

Objective: To determine and document that processing is lawful, with legal basis as per applicable jurisdictions, and with clearly defined and legitimate purposes.

Control Reference:

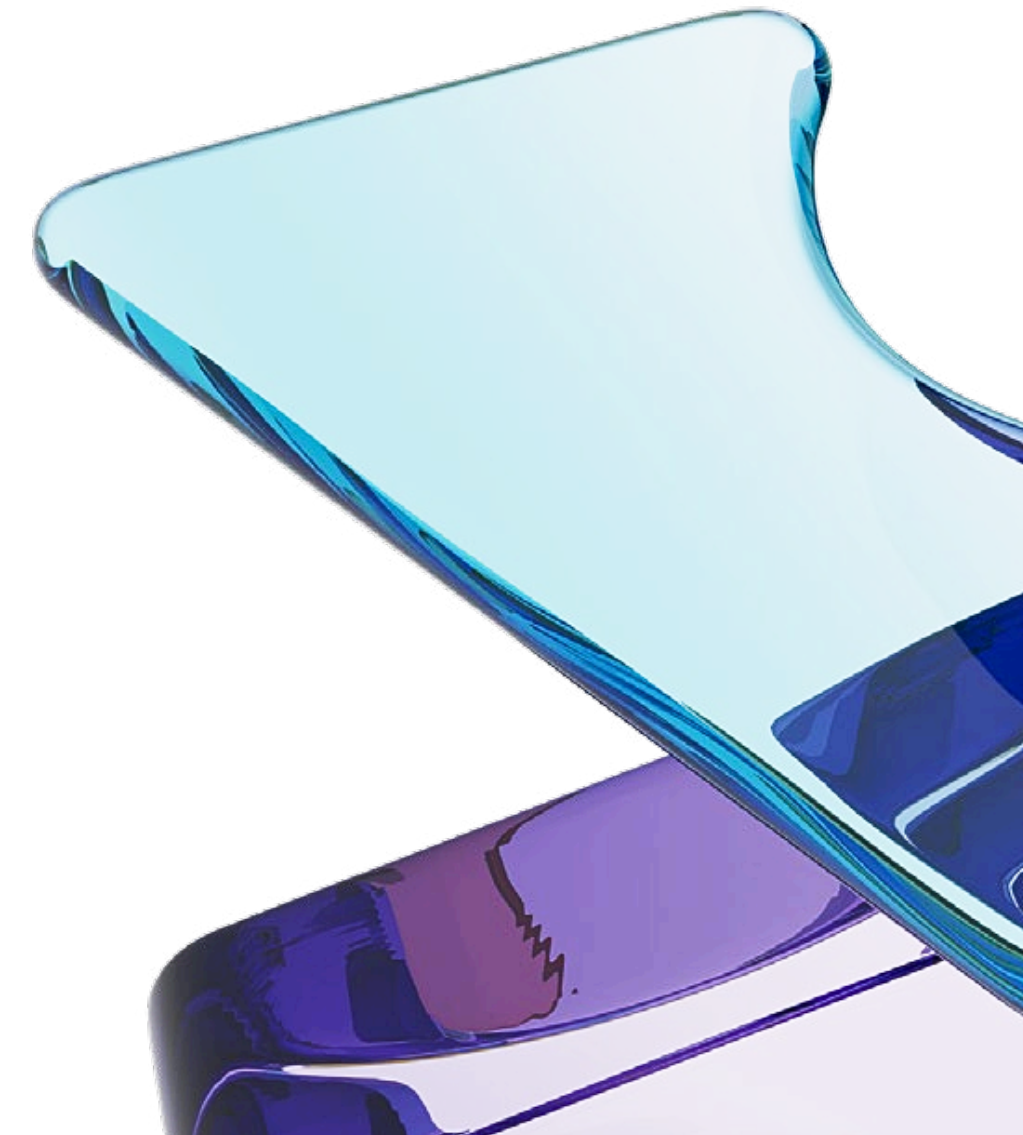
- A.2.2.2 Customer agreement
- A.2.2.3 Organization's purposes
- A.2.2.4 Marketing and advertising use
- A.2.2.5 Infringing instruction
- A.2.2.6 Customer obligations
- A.2.2.7 Records related to processing PII

Obligations to PII principals

Objective: To ensure that PII principals are provided with the appropriate information about the processing of their PII, and to meet any other applicable obligations to PII principals related to the processing of their PII.

Control Reference:

- A.2.3.2 Obligations to PII principals



A2 – Control Objective and control for PII Processors

Privacy by design and privacy by default

Objective:

To ensure that processes and systems are designed such that the collection and processing of PII (including use, disclosure, retention, transmission and disposal) are limited to what is necessary for the identified purpose.

Control Reference:

A.2.4.2 Temporary files

A.2.4.3 Return, transfer or disposal of PII

A.2.4.4 PII transmission controls

I sharing, transfer and disclosure

Objective:

To determine whether and document when PII is shared, transferred to other jurisdictions or third parties and/or disclosed in accordance with applicable obligations.

Control Reference:

A.2.5.2 Basis for PII transfer between jurisdictions

A.2.5.3 Countries and international organizations to which PII

can be transferred

A.2.5.4 Records of PII disclosure to third parties

A.2.5.5 Notification of PII disclosure requests

A.2.4.6 Legally binding PII disclosures

A.2.5.7 Disclosure of subcontractors used to process PII

A.2.5.8 Engagement of a subcontractor to process PII

A.2.5.9 Change of subcontractor to process PII

Example of Annex A

Table A.3 – Control Objective and control for PII Controllers and PII Processors

Security considerations for PII controllers and processors		
Objective: To ensure the security of PII processing.		
Control reference	Control title	Control
A.3.3	Policies for information security	Information security policies related to PII processing shall be defined, approved by management, published, communicated to and acknowledged by relevant personnel and relevant interested parties, and reviewed at planned intervals and if significant changes occur.
A.3.4	Information security roles and responsibilities	Information security roles and responsibilities related to PII processing shall be defined and allocated according to the organization needs.
A.3.5	Classification of information	Information shall be classified according to the information security needs of the organization, with consideration for PII, based on confidentiality, integrity, availability and relevant interested party requirements.

A3 – Control Objective and control for PII Controllers and PII Processors

Security consideration for PII controllers and processors

Objective:

To ensure the security of PII processing

Control Reference:

- A.3.3 Policy for information security
- A.3.4 Information security role and responsibilities
- A.3.5 Classification of information
- A.3.6 Labelling of information
- A.3.7 Information transfer
- A.3.8 Identity management
- A.3.9 Access Rights
- A.3.10 Addressing information security within supplier agreement

- A.3.11 Information security incident management planning and preparation
- A.3.12 Response to information incident
- A.3.13 Legal, statutory, regulatory and contractual requirement
- A.3.14 Protect of record
- A.3.15 Independent review of information security
- A.3.16 Compliance with policies, rules and standard for information security
- A.3.17 Information awareness, education, and training
- A.3.18 Confidentiality or nondisclosure agreement
- A.3.19 Clear desk and clear screen
- A.3.20 Store media
- A.3.21 Secure disposal or re-use of equipment
- A.3.22 User endpoint devices
- A.3.23 Secure authentication

A3 – Control Objective and control for PII Controllers and PII Processors

Information backup

A.3.24 Information backup

A.3.25 Logging

A.3.26 Use of cryptography

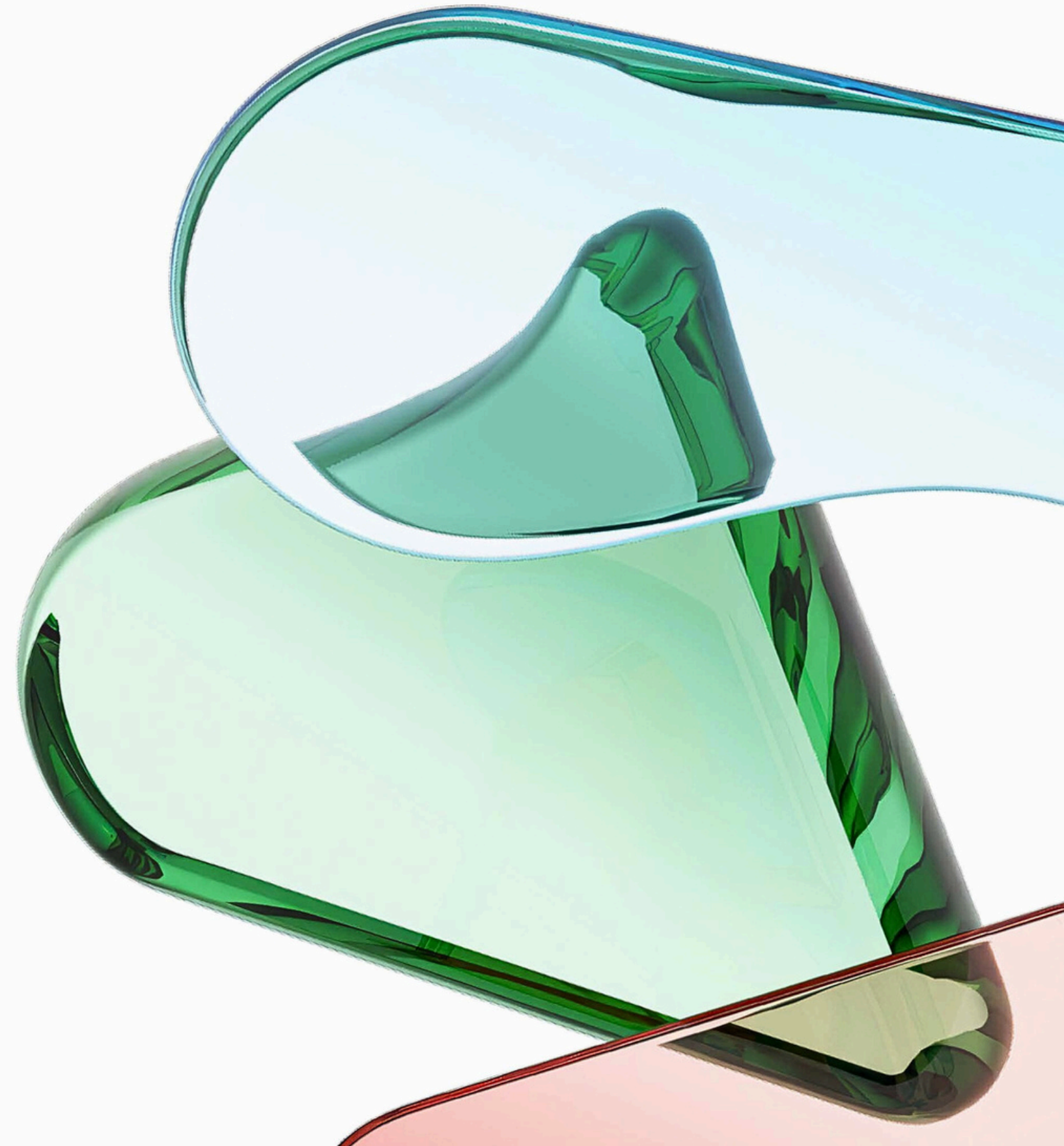
A.3.27 Secure Development Life cycle

A.3.28 Application security requirement

A.3.29 Secure system architecture and engineering
principle

A.3.30 Outsource development

A.3.31 Test information





***Annex B
Implementation guidance
for PII Controller and
PII Processors***



Annex B: Implementation guidance for PII Controller and PII Processors

B1. Implementation guidance for PII Controller

- Same as ISO/IEC 27701:2019 Req. 7

B2. Implementation guidance for PII Processor - Same as ISO/IEC 27701:2019 Req. 8

B3. Implementation guidance for PII Controller and PII Processors

- Security control guidance.
- It is covered implement guide for each control.





Annex C Mapping to ISO/IEC 29110

Annex C: Mapping for ISO/IEC 29110

Table C.1 — Mapping of controls for PII controllers and ISO/IEC 29100

Privacy principles of ISO/IEC 29100	Related controls for PII controllers
1. Consent and Choice	A.1.2.2 Identify and document purpose A.1.2.3 Identify lawful basis A.1.2.4 Determine when and how consent is to be obtained A.1.2.5 Obtain and record consent A.1.2.6 Privacy impact assessment A.1.3.5 Providing mechanism to modify or withdraw consent A.1.3.6 Providing mechanism to object to PII processing A.1.3.8 PII controllers' obligations to inform third parties
2. Purpose legitimacy and specification	A.1.2.2 Identify and document purpose A.1.2.3 Identify lawful basis A.1.2.6 Privacy impact assessment A.1.3.3 Determining information for PII principals A.1.3.4 Providing information to PII principals A.1.3.11 Automated decision making

Example

Table C.2 — Mapping of controls for PII processors and ISO/IEC 29100

Privacy principles of ISO/IEC 29100	Related controls for PII processors
1. Consent and choice	A.2.2.6 Customer obligations
2. Purpose legitimacy and specification	A.2.2.2 Customer agreement A.2.2.3 Organization's purposes A.2.2.4 Marketing and advertising use A.2.2.5 Infringing instruction A.2.3.2 Comply with obligations to PII principals
3. Collection limitation	N/A
4. Data minimization	A.2.4.2 Temporary files
5. Use, retention and disclosure limitation	A.2.5.4 Records of PII disclosure to third parties A.2.5.5 Notification of PII disclosure requests A.2.5.6 Legally binding PII disclosures
6. Accuracy and quality	N/A
7. Openness, transparency and notice	A.2.5.7 Disclosure of subcontractors used to process PII A.2.5.8 Engagement of a subcontractor to process PII A.2.5.9 Change of subcontractor to process PII



Annex D Mapping to the General Data Protection Regulation



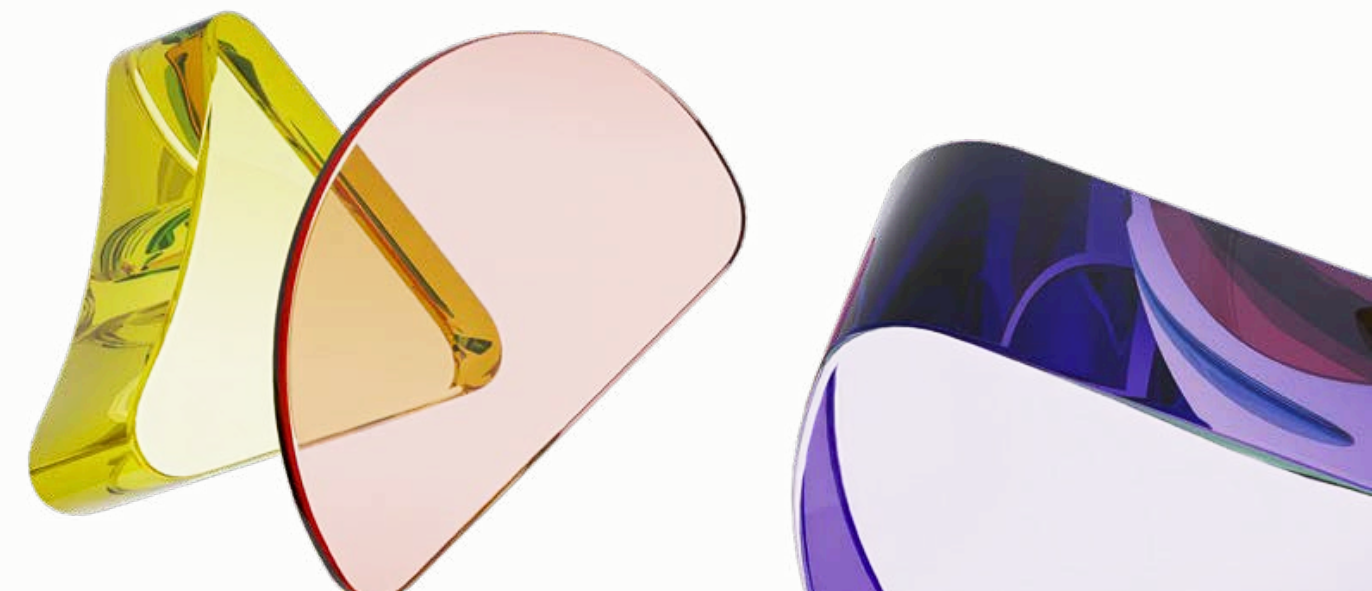
Annex D: Mapping to the General Data Protection Regulation

Table D.1 — Mapping of ISO/IEC 27701 structure to GDPR articles

Subclause of this document	GDPR article
4.1	(24)(3), (25)(3), (28)(5), (28)(6), (28)(10), (32)(3), (40)(1), (40)(2)(a), (40)(2)(b), (40)(2)(c), (40)(2)(d), (40)(2)(e), (40)(2)(f), (40)(2)(g), (40)(2)(h), (40)(2)(i), (40)(2)(j), (40)(2)(k), (40)(3), (40)(4), (40)(5), (40)(6), (40)(7), (40)(8), (40)(9), (40)(10), (40)(11), (41)(1), (41)(2)(a), (41)(2)(b), (41)(2)(c), (41)(2)(d), (41)(3), (41)(4), (41)(5), (41)(6), (42)(1), (42)(2), (42)(3), (42)(4), (42)(5), (42)(6), (42)(7), (42)(8)
4.2	(31), (35)(9), (36)(1), (36)(2), (36)(3)(a), (36)(3)(b), (36)(3)(c), (36)(3)(d), (36)(3)(e), (36)(3)(f), (36)(5)
4.3	(32)(2)
4.4	(32)(2)
6.1.2	(32)(1)(b), (32)(2)
6.1.3	(32)(1)(b), (32)(2)
5.2	(24)(2)
5.3	(27)(1), (27)(2)(a), (27)(2)(b), (27)(3), (27)(4), (27)(5), (37)(1)(a), (37)(1)(b), (37)(1)(c), (37)(2), (37)(3), (37)(4), (37)(5), (37)(6), (37)(7), (38)(1), (38)(2), (38)(3), (38)(4), (38)(5), (38)(6), (39)(1)(a), (39)(1)(b), (39)(1)(c), (39)(1)(d), (39)(1)(e), (39)(2)

Example

Subclause of this document	GDPR article
	(28)(3)(f), (28)(3)(g), (28)(3)(h), (30)(2)(d), (32)(1)(b)
B.3.14	(5)(2), (24)(2)
B.3.15	(32)(1)(d), (32)(2)
B.3.16	(32)(1)(d), (32)(2)
B.3.17	(39)(1)(b)
B.3.18	(5)(1)(f), (28)(3)(b), (38)(5)
B.3.19	(5)(1)(f)
B.3.20	(5)(1)(f), (32)(1)(a)
B.3.21	(5)(1)(f)
B.3.22	(5)(1)(f)
B.3.23	(5)(1)(f)
B.3.24	(5)(1)(f), (32)(1)(c)
B.3.25	(5)(1)(f)
B.3.26	(32)(1)(a)
B.3.27	(25)(1)
B.3.28	(5)(1)(f), (32)(1)(a)
B.3.29	(25)(1)



Annex E
Mapping to ISO/IEC
27018 and
ISO/IEC 29151

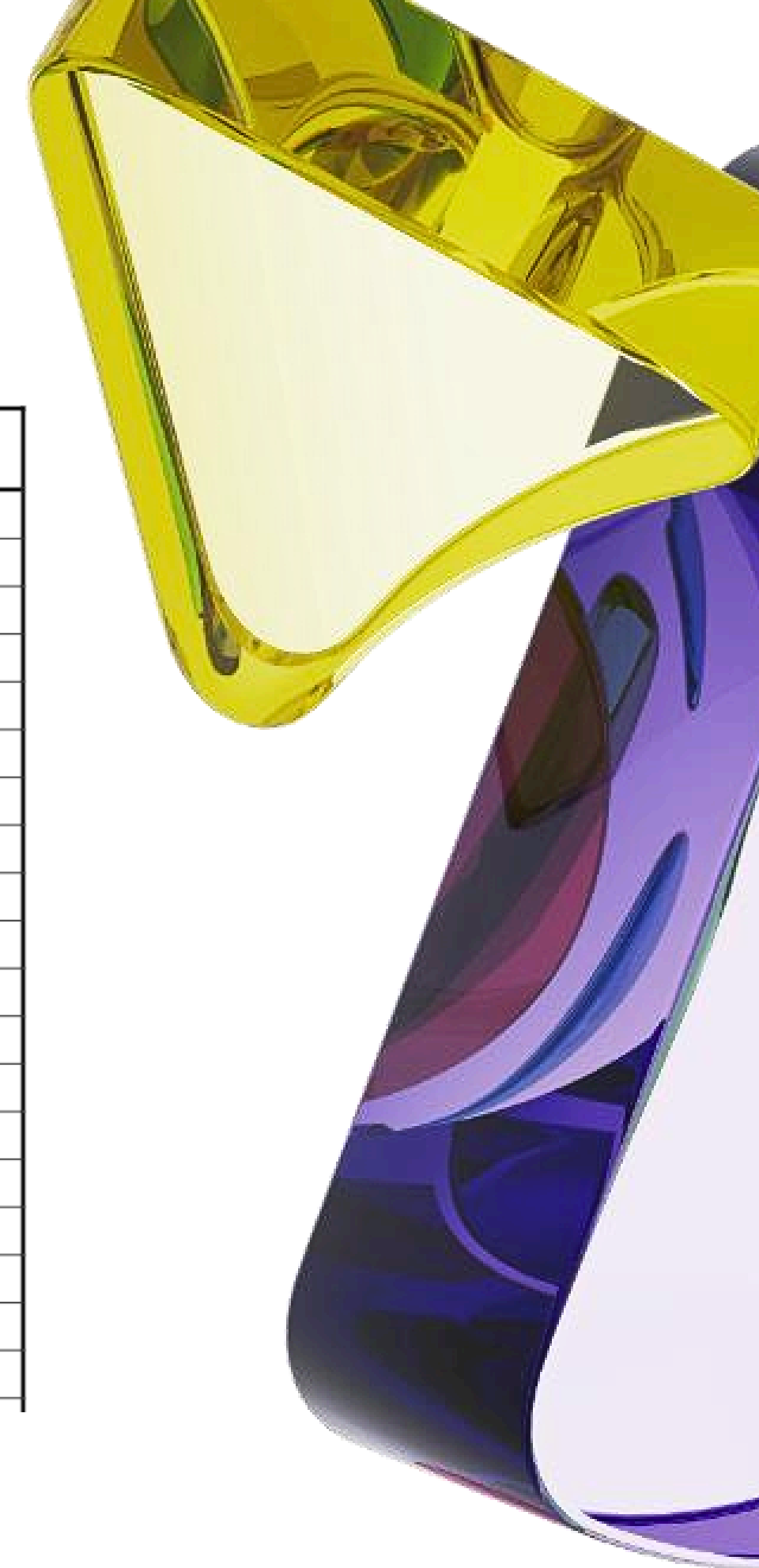


Annex E: Mapping to ISO/IEC 27018 and ISO/IEC 29151

Table E.1 — Mapping of ISO/IEC 27701 to ISO/IEC 27018 and ISO/IEC 29151

Subclause in this document	Subclause in ISO/IEC 27018	Subclause in ISO/IEC 29151
4	N/A	N/A
5	N/A	N/A
6	N/A	4.2
7	N/A	7.2.3
8	N/A	N/A
9	N/A	N/A
10	N/A	N/A
B.3.2	N/A	N/A
B.3.3, B.3.4, B.3.5, B.3.6, B.3.7, B.3.8, B.3.9, B.3.10, B.3.11, B.3.12, B.3.13, B.3.14, B.3.15, B.3.16	5.1.1, 6.1.1, 9.2.1, 16.1.1, 18.2.1, A.10.1, A.10.2, A.11.6, A.11.8, A.11.9, A.11.10, A.11.11	5, 8.1, 8.2, 9.2, 9.3, 18.2
B.3.17, B.3.18	7.2.2	N/A
B.3.19, B.3.20, B.3.21	11.2.7, A.11.2, A.11.4, A.11.5, A.11.13,	8.3, 11.1
B.3.22, B.3.23, B.3.24, B.3.25, B.3.26, B.3.27, B.3.28, B.3.29, B.3.30, B.3.31	7.2.2, 9.4.2, 10.1.1, 12.1.4, 12.4.1, 12.4.2, 13.2.1, A.11.1	9.4, 12.1, 12.2, 12.3, 12.4, 13.1, 13.2
B.1.2.2	N/A	A.4
B.1.2.3	N/A	A.4.1

Subclause in this document	Subclause in ISO/IEC 27018	Subclause in ISO/IEC 29151
B.1.2.7	N/A	A.11.3
B.1.2.8	N/A	N/A
B.1.2.9	N/A	N/A
B.1.3.2	N/A	A.10
B.1.3.3	N/A	N/A
B.1.3.4	N/A	A.9
B.1.3.5	N/A	N/A
B.1.3.6	N/A	N/A
B.1.3.7	N/A	A.10.1
B.1.3.8	N/A	N/A
B.1.3.9	N/A	N/A
B.1.3.10	N/A	N/A
B.1.3.11	N/A	N/A
B.1.4.2	N/A	A.5
B.1.4.3	N/A	N/A
B.1.4.4	N/A	A.8
B.1.4.5	N/A	N/A
B.1.4.6	N/A	A.7.1
B.1.4.7	N/A	A.7.2



Annex F
Correspondance with
ISO/IEC 27701:2019

Annex F: Correspondence with ISO/IEC 27701:2019

F1. Correspondence between control in this document and ISO/IEC 27701:2019

ISO/IEC 27701 control identifier	ISO/IEC 27701:2019 control identifier	Control name
A.3.3	6.2.1.1, 6.2.1.2	Policies for information security
A.3.4	6.3.1.1	Information security roles and responsibilities
N/A	6.3.1.2	Segregation of duties
N/A	6.4.2.1	Management responsibilities
N/A	6.3.1.3	Contact with authorities
N/A	6.3.1.4	Contact with special interest groups
N/A	New	Threat intelligence
N/A	6.3.1.5, 6.11.1.1	Information security in project management
N/A	6.5.1.1, 6.5.1.2	Inventory of information and other associated assets
N/A	6.5.1.3, 6.5.2.3	Acceptable use of information and other associated assets
N/A	6.5.1.4	Return of assets
A.3.5	6.5.2.1	Classification of information
A.3.6	6.5.2.2	Labelling of information
A.3.7	6.10.2.1, 6.10.2.2, 6.10.2.3	Information transfer
N/A	6.6.1.1, 6.6.1.2	Access control
A.3.8	6.6.2.1	Identity management
N/A	6.6.2.4, 6.6.3.1, 6.6.4.3	Authentication information
A.3.9	6.6.2.2, 6.6.2.5, 6.6.2.6	Access rights

A.3.10	6.12.1.1 6.12.1.2	Addressing information security within supplier agreements
N/A	6.12.1.3	Managing information security in the ICT supply chain
N/A	6.12.2.1, 6.12.2.2	Monitoring, review and change management of supplier services
N/A	New	Information security for use of cloud services
N/A	6.13.1.1	Information security incident management planning and preparation
A.3.11	6.13.1.4	Assessment and decision on information security events
A.3.12	6.13.1.5	Response to information security incidents
N/A	6.13.1.6	Learning from information security incidents
N/A	6.13.1.7	Collection of evidence
N/A	6.14.1.1, 6.14.1.2, 6.14.1.3	Information security during disruption
N/A	New	ICT readiness for business continuity
A.3.13	6.15.1.1, 6.15.1.5	Legal, statutory, regulatory and contractual requirements
N/A	6.15.1.2	Intellectual property rights
A.3.14	6.15.1.3	Protection of records
N/A	6.15.1.4	Privacy and protection of PII
A.3.15	6.15.2.1	Independent review of information security
A.3.16	6.15.2.2, 6.15.2.3	Compliance with policies, rules and standards for information security
N/A	6.9.1.1	Documented operating procedures
N/A	6.4.1.1	Screening
N/A	6.4.1.2	Terms and conditions of employment
A.3.17	6.4.2.2	Information security awareness, education and training
N/A	6.4.2.3	Disciplinary procedures
N/A	6.4.3.1	Responsibilities after termination or change of employment
A.3.18	6.10.2.4	Confidentiality or non-disclosure agreements
N/A	6.3.2.2	Remote working
N/A	6.13.1.2, 6.13.1.3	Information security event reporting
N/A	6.8.1.1	Physical security perimeter
N/A	6.8.1.2, 6.8.1.6	Physical entry

Annex F: Correspondence with ISO/IEC 27701:2019

F1. Correspondence between control in this document and ISO/IEC 27701:2019

N/A	6.10.1.2	Security of network services
N/A	6.10.1.3	Segregation of networks
N/A	New	Web filtering
A.3.26	6.7.1.1, 6.7.1.2	Use of cryptography
A.3.27	6.11.2.1	Secure development life cycle
A.3.28	6.11.1.2, 6.11.1.3	Application security requirements
A.3.29	6.11.2.5	Secure system architecture and engineering principles
N/A	New	Secure coding
N/A	6.11.2.8, 6.11.2.9	Security testing in development and acceptance
A.3.30	6.11.2.7	Outsourced development
N/A	6.9.1.4, 6.11.2.6	Separation of development, testing and production environments
N/A	6.9.1.2, 6.11.2.2, 6.11.2.3, 6.11.2.4	Change management
A.3.31	6.11.3.1	Test information
N/A	6.9.7.1	Protection of information systems during audit testing

N/A	6.8.1.3	Securing offices, rooms and facilities
N/A	New	Physical security monitoring
N/A	6.8.1.4	Protecting against physical and environmental threats
N/A	6.8.1.5	Working in secure areas
A.3.19	6.8.2.9	Clear desk and clear screen
N/A	6.8.2.1	Equipment siting and protection
N/A	6.8.2.6	Security of assets off-premises
A.3.20	6.5.3.1, 6.5.3.2, 6.5.3.3, 6.8.2.5	Storage media
N/A	6.8.2.2	Supporting utilities
N/A	6.8.2.3	Cabling security
N/A	6.8.2.4	Equipment maintenance
A.3.21	6.8.2.7	Secure disposal or re-use of equipment
A.3.22	6.3.2.1, 6.8.2.8	User endpoint devices
N/A	6.6.2.3	Privileged access rights
N/A	6.6.4.1	Information access restriction
N/A	6.6.4.5	Access to source code
A.3.23	6.6.4.2	Secure authentication
N/A	6.9.1.3	Capacity management
N/A	6.9.2.1	Protection against malware
N/A	6.9.6.1	Management of technical vulnerabilities
N/A	New	Configuration management
N/A	New	Information deletion
N/A	New	Data masking
N/A	New	Data leakage prevention
A.3.24	6.9.3.1	Information backup
N/A	6.14.2.1	Redundancy of information processing facilities
A.3.25	6.9.4.1, 6.9.4.2, 6.9.4.3	Logging
N/A	New	Monitoring activities
N/A	6.9.4.4	Clock synchronization
N/A	6.6.4.4	Use of privileged utility programme(s)
N/A	6.9.5.1, 6.9.6.2	Installation of software on operational systems
N/A	6.10.1.1	Network security

Annex F: Correspondence with ISO/IEC 27701:2019

F2. Correspondence between control in ISO/IEC 27701:2019 and this document



Table F.2 — Correspondence between controls in ISO/IEC 27701:2019 and controls in this document

ISO/IEC 27701:2019 control identifier	ISO/IEC 27701 control identifier	Control name according to ISO/IEC 27701:2019
6.2.1.1	A.3.3	Policies for information security
6.2.1.2	A.3.3	Review of policies for information security
6.3.1.1	A.3.4	Internal security roles and responsibilities
6.3.1.2	N/A	Segregation of duties
6.3.1.3	N/A	Contact with authorities
6.3.1.4	N/A	Contact with special interest groups
6.3.1.5	N/A	Information security in project management
6.3.2.1	A.3.22	Mobile device policy

Example

6.3.2.2	N/A	Teleworking
6.4.1.1	N/A	Screening
6.4.1.2	N/A	Terms and conditions of employment
6.4.2.1	N/A	Management responsibilities
6.4.2.2	A.3.17	Information security awareness, education and training
6.4.2.3	N/A	Disciplinary procedures
6.4.3.1	N/A	Termination or change of employment responsibilities
6.5.1.1	N/A	Inventory of assets
6.5.1.2	N/A	Ownership of assets
6.5.1.3	N/A	Acceptable use of assets
6.5.1.4	N/A	Return of assets
6.5.2.1	A.3.5	Classification of information
6.5.2.2	A.3.6	Labelling of information
6.5.2.3	N/A	Handling of assets
6.5.3.1	A.3.20	Management of removable media
6.5.3.2	A.3.20	Disposal of media

แนวทางการปรับ เปลี่ยนผ่านไปสู่ **ISO/IEC 27001** ***New version***

*(Draft for public comment
02 July 2024)*



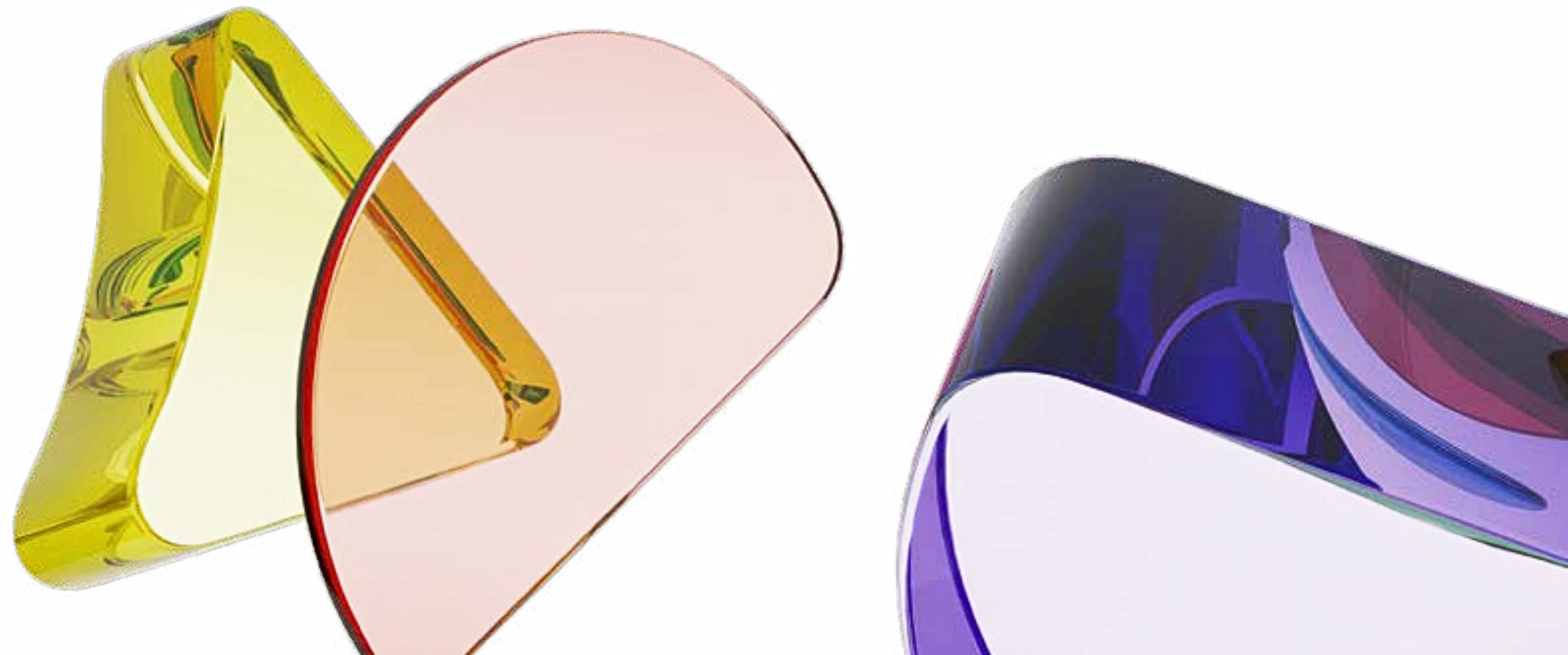
แนวทางการปรับเปลี่ยนผ่านไปสู่อุ *ISO/IEC 27701 New version*

Organization:

1. Waiting for public the standard
2. Study / Training new version requirement
3. Conduct gap analysis
4. Implement to close gap
5. Internal audit
6. Management review
7. Inform to BSI for transition to new version

BSI:

1. Waiting for public the standard
2. Study new version requirement
3. Qualify auditors/ Trainers for new version
4. Waiting for Accreditation Body (AB) approve to BSI for audit new version
5. It can conduct to certify new version



" Q&A

ทบทวนและถามคำถาม



สแกน QR code เป็นเพื่อนกับเราใน Line official ของ BSI
เพื่อไม่ให้พลาดข่าวสารข้อมูลที่เป็นประโยชน์ในสายอาชีพของท่าน

- Free webinars
- Tool และบทความดีๆ

bsi