A HOLISTIC APPROACH TO PRIVACY COMPLIANCE

22 Jan 2024

Speaker

Chris YAU, ***CISA, CISM, CDPSE, MHKCS***

Deputy Director, Products and Services Development, SGS

- Mr. Yau is the head of the new development and operations team at SGS Hong Kong Limited, responsible for adopting and transforming new standards into executable assessment and training services in the Asia Pacific region. He is a qualified lead auditor in QEHS, information security, personal data privacy, IT service management, supply chain security, and hazardous substance process management. He has over 20 years of audit experiences covering 800+ organizations.

PRIVACY IS MORE THAN JUST SECURITY

COMMON PITFALLS

- Many people regard personal data privacy as data security only
- They thought *data privacy* is about
  - Data is stored securely (password protected or encrypted)
  - Not accessible by unauthorized persons
  - Not transferred to 3rd party
- Treat personal data as simply an asset in information security management

5 min GDPR review:
Data processing principles

	Principles	
1	Lawfulness, Fairness, and Transparency	Personal data must be processed lawfully, fairly and transparently
2	Purpose Limitation	Personal data can only be collected for specified, explicit and legitimate purposes
3	Data minimization	Personal data must be adequate, relevant and limited to what is necessary for processing
4	Accuracy	Personal data must be accurate and kept up to date
5	Storage limitation	Personal data must be kept in a form such that data subject can be identified only as long as needed for processing
6	Integrity and confidentiality	Personal data must be processed in a manner that ensure its security

These areas cannot be helped by IT / security technologies alone

5 min GDPR review: Data subject rights

	Rights	
1	The right to be informed (Articles 13-14)	To know the data has been obtained
2	The right of access (Article 15)	To see what the controller / processes has
3	The right to rectification (Article 16)	To make sure the data is accurate
4	The right to erasure (“right to be forgotten”) (Article 17)	To remove all data obtained or processed
5	The right to restrict processing (Article 18)	To stop processing of data because of data accuracy, purpose of processing, and lawfulness of processing is demonstrated.
6	The right to data portability (Article 20)	To obtain obtained or processed data in usable form.
7	The right to object (Article 21)	To object to processing for direct marketing purposes
8	Rights in relation to automated decision making and profiling (Article 22)	To object to profiling

IT technologies is essential to automate some of these, but they need the compliance team to advise the detailed legal requirements and **what data** to extract.

5 min GDPR review:
Other important requirements

	Requirements	
1	Data processing agreement (Article 28)	Processing by a processor shall be governed by a contract or a legal act
2	Security of processing (Article 32)	The information security protection of the PII
3	Data protection impact assessment (Article 35-36)	To make sure the data is accurate
4	Transfer of PII to 3rd country (Articles 44-50)	Cross-border data transfer
5	Binding corporate rules (Article 46)	A legal-binding agreement between the controller (e.g. a phone app) and the processor (e.g. cloud provider)
6	Data breach notification (Article 33-34)	Inform the authority when there is a data breach
7	Certification (Article 42-33)	The EU EDPB may endorse schemes proposed to the EDPB

PRIVACY *DATA SECURITY* RISKS VS PRIVACY *PROCESSING* RISKS

CIA of privacy data

- Breach of PII data by hackers;
- Loss of PII database due to hard disc failure;
- Loss of a USB drive that contains PII data;
- Loss of a laptop used by HR staff;
- Transfer of PII data without encryption.

Processing of privacy data

- Transfer of PII to an overseas subsidiary or outsourced data center
  - Cross-border PII transfer
- Subcontracting marketing of a mass mailing to a vendor
  - Data processing agreement?
- Use of a cloud-based software to handle pay-roll
  - Where is the “cloud”?
  - Any sub-processor?

CIA = confidentiality, integrity and availability

EXAMPLES OF PRIVACY CONTROLS TO INFORMATION SECURITY

Privacy considerations

- How to delete personal data in your backup? (“Right to be forgotten”)
- Your privacy policy (keep for 60 days only) vs backup frequency (you keep a yearly backup!)

Backup

Application development

Privacy considerations

- Application designed to follow the processing principles (data minimization, data retention period, etc)
- Awareness on “special categories of data”?
- Awareness and competency on the skill of de-identification / pseudo-anonymization / encryption of PII?

Suppliers processing PII

Privacy considerations

- Data processing agreement?
  - Overseas supplier?
  - Data returned upon termination of contract?
  - “Right to be audited” clause?

Incident management

Privacy consideration

- Is data breach considered an incident?
  - Many incident management policies only define events that affect production or data loss as incidents.
- Incident reports to authority timely? (GDPR 72hrs)

EXAMPLES OF PRIVACY CONTROLS FOR PII CONTROLLER

Privacy consideration

- How are consents obtained?
  - Channel?
  - Date and time stamp?
  - Purpose?
- Provided opportunity to withdraw consent?
- Bundled with conditions?

Informed Consent
Given complex data flows, informed consent is increasingly challenging – so an alternative is needed: An accountability governance model incorporating ethics and respectful data use is a compelling substitute or complement.

Privacy considerations

- Are PII being transferred to other countries (e.g. database in other countries)?
  - What's the legal basis?
  - What are the security controls in place?

Cross-border data transfer

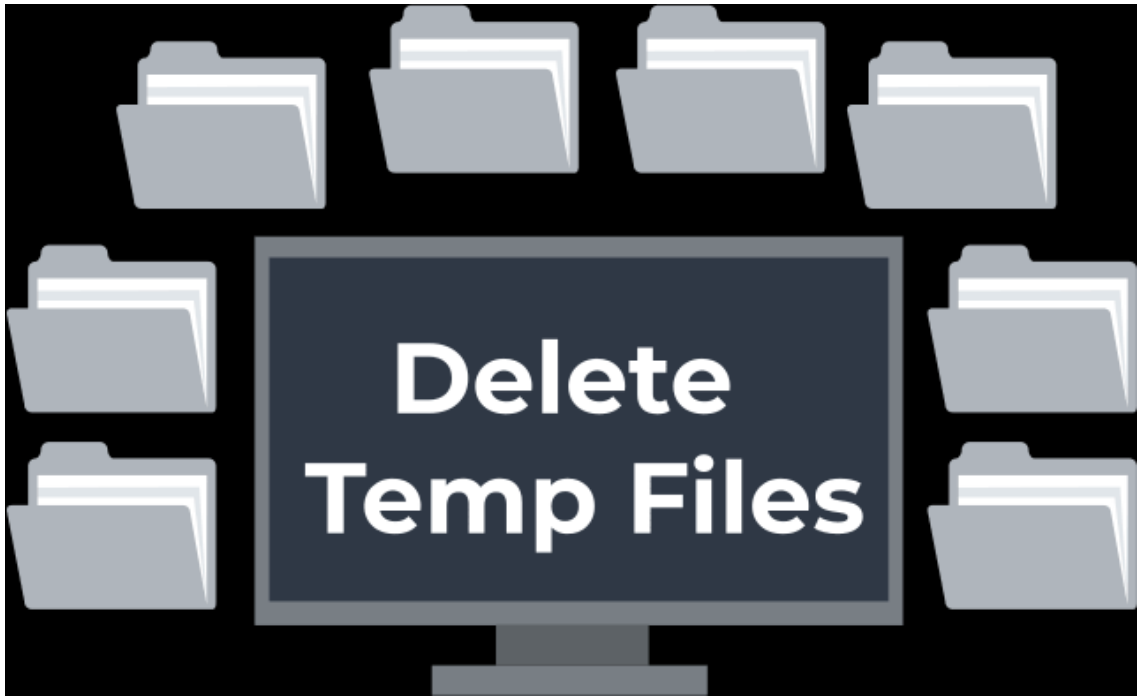
EXAMPLES OF PRIVACY CONTROLS TO PII PROCESSOR

Privacy considerations

- Will the PII collected be used for marketing or advertising purposes without the consent of the PII subject?
- Will the consent be a condition for receiving the service?

Marketing and advertising use

Handling of temporary files



Privacy consideration

- Temporary files containing PII are sometimes generated by users or by applications. These files may be stored at locations that are accessible by unauthorized personnel.

SUMMARY

Privacy is not just about security.

Information security alone is insufficient in managing privacy.

A framework to manage PII is needed.

PRIVACY NEEDS TO BE MANAGED SYSTEMATICALLY

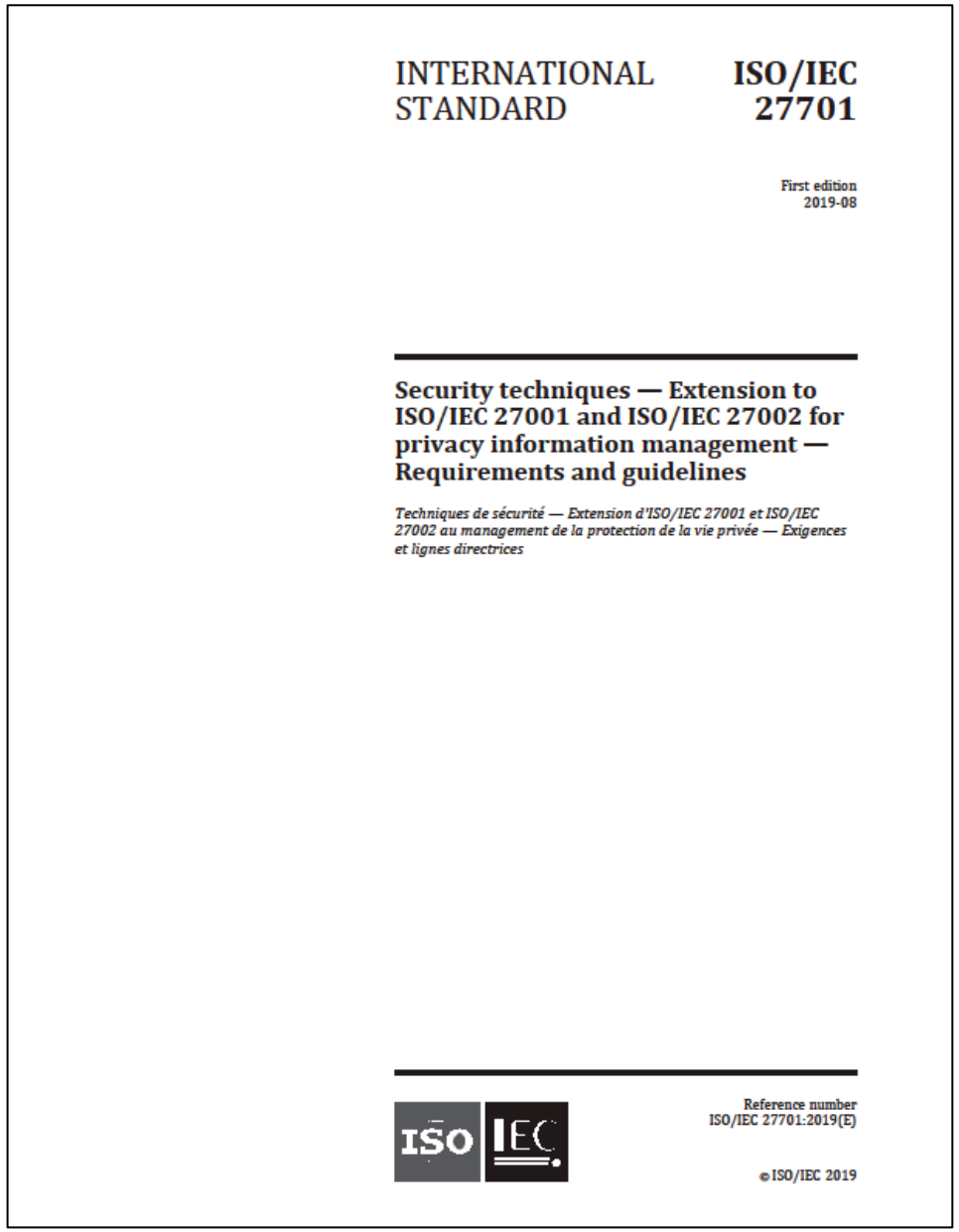
- Privacy is a collaborative effort of IT, Compliance team, and others.
- Privacy management should be an integral part of an organization's overall management strategy

- Many issues need to be managed systematically, e.g.
  - Documents (e.g. privacy notice, privacy policies, privacy data register, etc) need to be reviewed and updated
  - Staff (DPO, frontlines, DSAR CRM, etc) need to be regularly trained
  - Governance structure (top management involvement, roles and responsibilities, training and awareness)
  - Effectiveness monitoring (KPI, internal audit, external assessment, etc)

ISO/IEC 27701:2019

PRIVACY INFORMATION MANAGEMENT SYSTEM

- Released in Aug 2019
- Specifies requirements and provide guidance for establishing, implementing, and continually improving a PIMS in the form of an extension to ISO/IEC 27001 and ISO/IEC 27002
- Can be used by PII controllers (including joint controllers) and PII processors (including subcontractors to PII processors)
- Mixture of requirements and guidelines



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

ISO IEC

Reference number
ISO/IEC 27701:2019(E)

PRIVACY INFORMATION MANAGEMENT SYSTEM (PIMS)

ISO/IEC 27701 is designed to work with ISO/IEC 27001 to form a complete Privacy Information Management System

Organization must first possess an ISO/IEC 27001 information security management system

ISO/IEC 27701 WORKS WITH ISO/IEC 27001

A complete Privacy Information Management System (PIMS)

Ensure the processing of personal data meets the principles and data subject rights

ISO/IEC 27701

- 5 clauses amended with PIMS-related requirements
- 32 (out of 114) amended with privacy requirements
- Annex A: 31 controls for PII controller
- Annex B: 18 controls for PII processor

ISO/IEC 27001

- Clause 4 - 10
- Annex A: 114 controls

Ensure the confidentiality (C), integrity (I) and availability (A) of personal data.

TWO MANDATORY ANNEXES

BENEFITS OF CERTIFYING TO ISO/IEC 27701

- An objective way to demonstrate your organization's effort, capability, and results of meeting all applicable customer and regulatory privacy requirements.
- An achievement to show your current and future customers that your privacy management has attained world-class benchmark
- An opportunity to enhance your organization's privacy competence and awareness by having a 3rd party monitoring.
- An attraction to more businesses because of your organization's demonstration to respect privacy.

Contact:

Denis Ho

Business Development Manager and ISO 27001, TISAX, ISO/SAE 21434 auditor

Tel: 9409-2779

Email: denis.ho@sgs.com