nqa.
a kiwa company

Privacy Information Management & ISO 27701:2019

Dylan Harvie
02.06.2025

OUR PURPOSE

IS TO HELP CUSTOMERS DELIVER PRODUCTS THE WORLD CAN

TRUST

NQA is a world leading certification body with global operations.

NQA specialises in certification in high technology & engineering sectors.

LONDON
BOSTON
SHANGHAI
BANGALORE

AMERICA'S NO.1

Certification body in **Aerospace** sector

TOP 3 IN THE UK

ISO 9001, ISO 14001, ISO 45001, ISO 27001

CHINA'S NO.1

Certification body in **Automotive** sector

GLOBAL NO.1

Certification body in **telecommunications & Automotive** sector

GLOBAL NO.3

Certification body in **Aerospace** sector

UK'S NO.2

Certification body in **Aerospace** sector

Who is ISO 27701 for?

KEY POINTS:

- UK organisations/non-UK organisations.
- Existing/potential NQA clients with ISO 27001 or other information security related standards.
- Organisations looking to gain ISO 27701 certification.

What is ISO 27701:2019?

KEY POINTS:

- Currently, an international Privacy Information Management System (PIMS) standard that extends ISO/IEC 27001 & ISO/IEC 27002 to include privacy management.

- To establish, implement, maintain & continuously improve a Privacy Information Management System.

- Why privacy matters.
    - Enhances information security management with data privacy controls.
    - Supports compliance with regulations like GDPR, DPA & others.
    - Helps organisations to manage Personally Identifiable Information (PII) under its remit.

Relationship with other ISO Standards

KEY POINTS:

- ISO 27001 – Information Security Management Systems (ISMS)
- ISO 27002 – Code of Practice for Information Security Controls
- ISO 29100 – Privacy Framework
- ISO 29101 – Privacy Architecture Framework
- ISO 27018 – Protection of PII in Public Clouds (for processors)
- ISO 29134 – Privacy Impact Assessment Guidelines
- ISO 27017 – Cloud Security Controls
- ISO 9001 – Quality Management Systems (QMS)

Transition

KEY POINTS:

- ISO 27701:2025 is currently under review & due for release later this year.
  - It was due for release in Q1, but we are now in Q2 & still waiting.
  - It will transition from an extension to ISO 27001 to be a standalone ISO standard; comparable to other Annex SL standards.
  - The new standard will permit organisations to operate an autonomous PIMS without also having to implement an ISMS.

- Key changes to be expected.
  - Standalone PIMS implementation.
  - Integration with ISO 42001:2024 (AIMS).
  - Enhanced risk management approach.
  - Sector-specific applicability.
  - AI-specific governance & control mechanisms.

Application

KEY POINTS

The implementation of ISO 27701:2019 applies to:

•Personal information (PII) Controllers (organizations that determine how data is used).

•Personal information (PII) Processors (organizations that process data on behalf of others).

•Organizations acting as both Personal information (PII) Controllers & Processors

Requirements Overview

- Certification readiness:
  Must already be certified to ISO 27001 as this is an extension.
- Extension of ISMS to PIMS:
  Organisations must build on their existing ISMS framework to include privacy specific requirements.

- Privacy-specific controls:
  Controls for personal information controllers &/or processors.
- Privacy governance & management:
  A defined privacy policy aligned to business & regulatory requirements.
  Assigned roles & responsibilities.
  Privacy in risk management.
  governance & management:

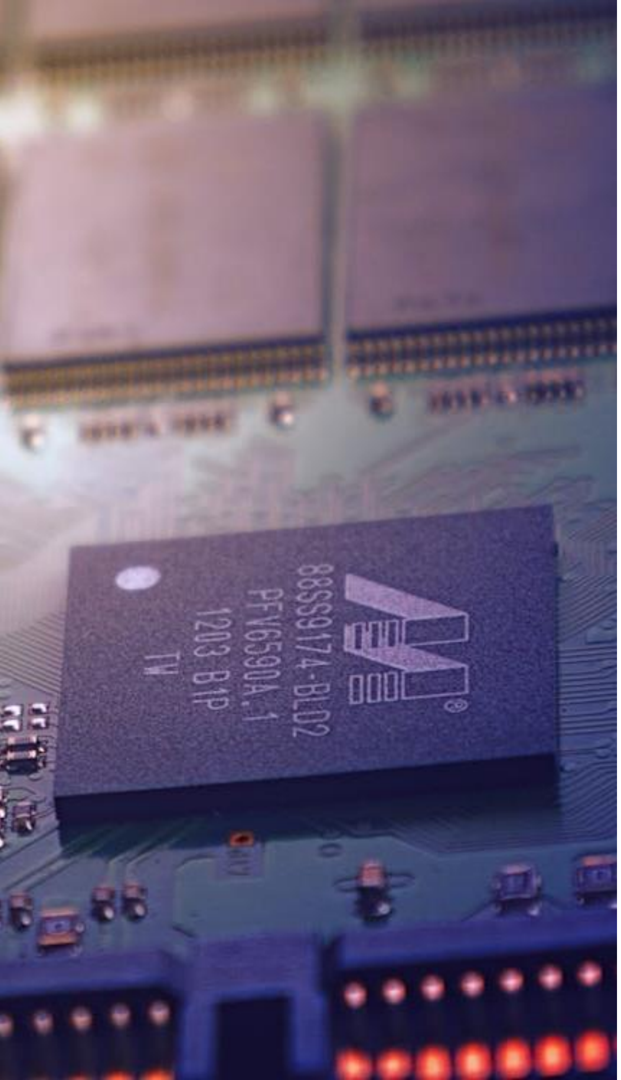
Requirements Overview

- Operational privacy controls:
  Controls aligned to privacy legislation.

- Documentation & record-keeping.
  Risk/impact assessments, training records, contracts & agreements.

Continued Improvement

Training
Internal Process
Record Keeping
Identify Controller Requirements



Annex Controls

The only requirements of the standard are outlined in Clause 5; all other clauses indicate guidance.

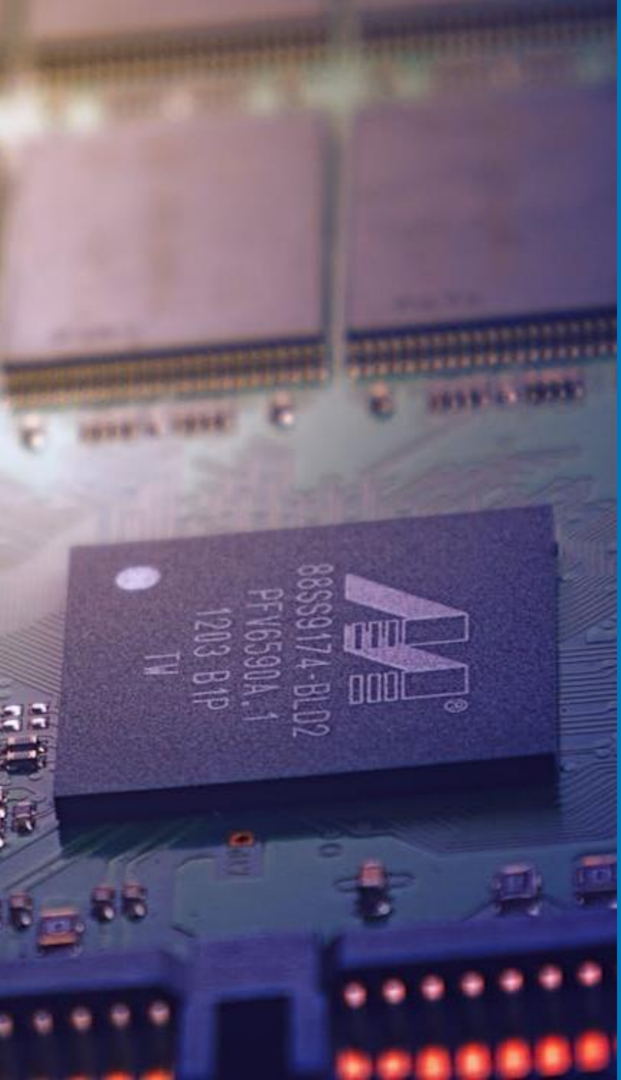
Annex A: Personal Information Controller

- Conditions for data processing
  Consent, reasons for processing, contracts, impact assessments.

- Obligations to principals
  Determining & fulfilling obligations, objections or consent withdrawals, data handling & decision-making.

- Privacy design by default.
  Limiting collection & processing, accuracy, retention, deletion, disposal & transmission.

- Sharing, transfer & disclosure.
  Transfer of data between jurisdictions, records of transfer & records of disclosure.



Annex Controls

The only requirements of the standard are outlined in Clause 5; all other clauses indicate guidance.

Annex B: Personal Information Processor

- Conditions for data processing

  Customer agreement, purpose, marketing use, infringements, customer obligations & records.

- Obligations to PII principals

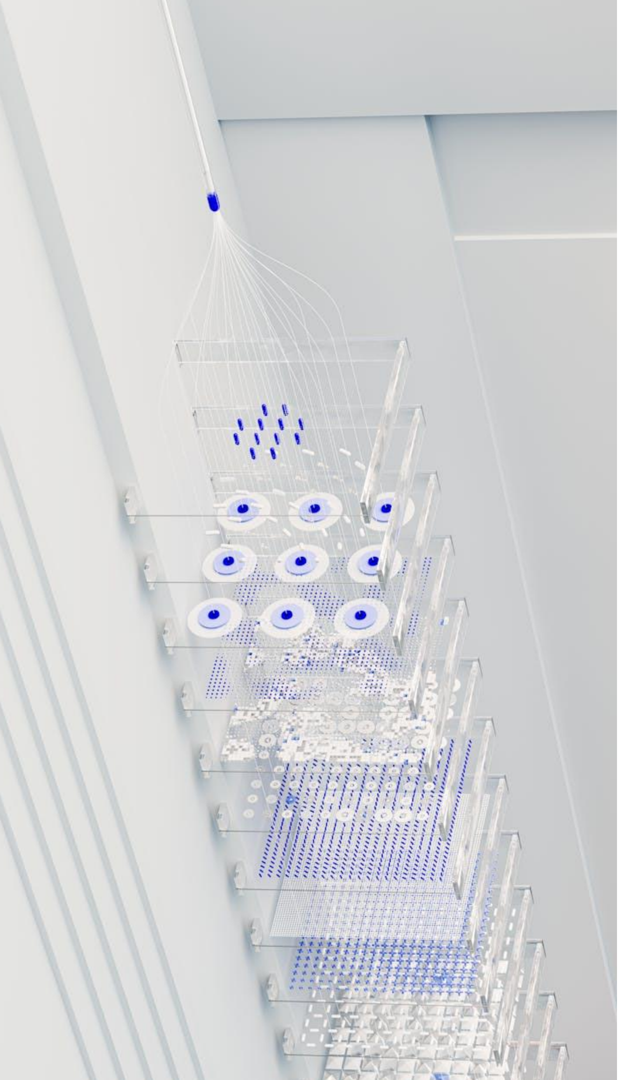
  Documented obligations to principals.

- Privacy design by default.

  Temporary files, return, transfer, disposal & transmission of personal information .

- Sharing, transfer & disclosure.

  Reasons for transfer, disclosure to third-parties, notification requests, change or engagement with subcontractors.



Benefits to your Organisation

KEY POINTS

1. Enhanced data privacy.

2. Demonstrable accountability & trust.

3. Improved international market access.

4. Integration with existing ISMS.

5. Risk management & privacy by design.

6. Structured privacy roles & responsibilities.

7. Competitive advantage.

8. Audit readiness.

CONCLUSION

CERTIFICATION & TRAINING SERVICES

We specialize in management systems certification for:

QUALITY

AEROSPACE (QUALITY)

AUTOMOTIVE (QUALITY)

SUSTAINABILITY

ENERGY

HEALTH & SAFETY

INFORMATION RESILIENCE

FOOD SAFETY

RISK MANAGEMENT

MEDICAL DEVICES

nqa.
a kiwa company

TRAINING OFFERED

STANDARD	TRAINING
ISO 9001	Quality Internal Auditor Training – 9th June
ISO 45001	Health & Safety Lead Auditor Conversion Training – 10th June
ISO 14001	Environmental Lead Auditor Training – 16th June
ISO 50001	Energy Lead Auditor Conversion Training – 23rd June

FURTHER SUPPORT

Call
0800 052 2424

Email:
training@nqa.com

Visit LinkedIn
@NQA

To find out more information on verification, certification, the training we offer or to receive top class support please get in touch.

Visit our website:
www.nqa.com

Check out our latest blogs
nqa.com/blog

Sign up to our e-zine, InTouch:
nqa.com/signup

nqa.
Sustainability Simplified
Podcast
NQA's Sustainability Simplified
NQA Global Certification Body

Q&A