Centre for Information Policy Leadership (CIPL) Webinar on ISO 27701 and CIPL’s Accountability Framework

29 January 2020
Nathalie Laneret
Director of Privacy Policy, CIPL
N Laneret@HuntonAK.com

Brian Philbrook
Privacy Counsel, OneTrust
BPhilbrook@OneTrust.com

Florian Thoma
Senior Director of Global Data Privacy, Accenture
Florian.Thoma@Accenture.com
Agenda

- 11:30  Introduction to Accountability and Certifications
- 11:40  What is ISO 27701 and what are its benefits?
- 12:00  Program Preparation and Getting Certified
- 12:20  ISO 27701 mapped to CIPL’s Accountability Framework
- 12:25  Q&A
- 12:30  End of Webinar
Introduction to Accountability & Certifications
A Global Privacy and Security Think Tank

ABOUT US
• The Centre for Information Policy Leadership (CIPL) is a global privacy and security think tank
• Based in Washington, DC, Brussels and London
• Founded in 2001 by leading companies and Hunton Andrews Kurth LLP
• CIPL works with industry leaders, regulatory authorities and policy makers to develop global solutions and best practices for data privacy and responsible use of data to enable the modern information age
Implementing Accountability

Accountability requires comprehensive privacy programs that translate legal requirements into risk-based, verifiable and enforceable corporate practices and controls.

Organizations must be able to demonstrate accountability – internally and externally.

Accountability is not static, but dynamic, reiterative and a constant journey.

Company values and business ethics shape accountability.

Effective Compliance and Protection for Individuals

Leadership and Oversight

Risk Assessment

Policies and Procedures

Transparency

Training and Awareness

Response and Enforcement

Monitoring and Verification
# Accountability – Examples of Content of Privacy Management Programs

## Leadership and Oversight
- Tone from the top
- Executive oversight
- Data privacy officer/office of oversight and reporting
- Data privacy governance
- Privacy engineers
- Internal/External Ethics Committees

## Risk Assessment
- At program level
- At product or service level
- DPIA for high risk processing
- Risk register
- Risk to organizations
- Risk to individuals
- Records of processing

## Policies and Procedures
- Internal privacy rules based on DP principles
- Information security
- Legal basis and fair processing
- Vendor/processor management
- Procedures for response to individual rights
- Other (e.g. Marketing rules, HR rules, M&A due diligence)
- Data transfers mechanisms
- Privacy by design
- Templates and tools for PIA
- Crisis management and incident response

## Transparency
- Privacy policies and notices to individuals
- Innovative transparency – dashboards, integrated in products/apps, articulate value exchange and benefits, part of customer relationship
- Information portals
- Notification of data breaches

## Training and Awareness
- Mandatory corporate training
- Ad hoc and functional training
- Awareness raising campaigns and communication strategy

## Monitoring and Verification
- Documentation and evidence - consent, legitimate interest and other legal bases, notices, PIA, processing agreements, breach response
- Compliance monitoring and testing - verification, self-assessments and audits
- Seals and certifications

## Response and Enforcement
- Individual requests and complaints-handling
- Breach reporting, response and rectification procedures
- Managing breach notifications to individuals and regulators
- Implementing response plans to address audit reports
- Internal enforcement of non-compliance subject to local laws
- Engagement/Co-operation with DPAs

Organizations must be able to **demonstrate their own implementation** - internally and externally
Accountability – What it is and What it is not

What it is

➢ Comprehensive
  • Comprehensive internal program giving effect to DP requirements
  • Verifiable, demonstrable and enforceable data protection commitment, infrastructure and controls

➢ Relevant
  • Relevant and scalable for all organizations
  • Private and public sector; large multinationals and SMEs; controllers and processors

➢ Consistent
  • Consistent with other areas of corporate law and governance and duty of care
  • Anti-bribery; anti-money laundering; export controls; Sarbanes-Oxley; Sustainability; Fiduciary duty

➢ Demonstrable
  • Internally: Executive leadership; Board of Directors; shareholders
  • Externally: Business partners; regulators; individuals; civil society

➢ Effective
  • Corporate Digital Responsibility fit for 21st century
  • Delivers effective protection for individuals and data
  • Enables responsible use, sharing and flows of data and innovation

What it is not

➢ Self Regulation
  • Sit on top of and in addition to legal requirements - it does not replace them (co-regulation)
  • Accountability operationalizes legal rules and delivers legal compliance

➢ Carte Blanche to use data
  • Requires organizations to implement all applicable DP norms and be able to demonstrate that implementation

➢ Self serving tool
  • Provides also benefits for regulators, individuals and society

➢ An excuse for failure
  • Minimizes the risks of breaches, and requires organizations to be prepared, responsive and responsible when they occur
  • Can be a mitigating factor in enforcement, but it does not give organizations a free pass
Examples of Privacy Management Frameworks

- Corporate Privacy Programs
- Binding Corporate Rules (BCR)
- APEC Cross Border Privacy Rules (CBPR)
- Codes of Conduct
- Certifications & Seals
- ISO Standards
What is ISO 27701 and what are its benefits?
### PIMS is Privacy extension to ISO 27001

Establishing, implementing, maintaining and continually improving a PIMS in the form of an extension to ISO 27001 for privacy management within the context of the organization.

### PIMS-specific requirements and guidance

A privacy information management system (PIMS) expands upon the ISMS and addresses the protection of privacy as potentially affected by the processing of PII.

### Extended interpretation

Where "information security" is used in ISO 27001 and 27002, "information security and privacy“ applies instead.
The Design Intent of ISO 27701

A universal set of operation controls to reconcile privacy regulations into practice
# Core Components

<table>
<thead>
<tr>
<th><strong>Context &amp; Scope</strong></th>
<th>Determine context or organization and scope of certification Two sets of controls: Controller and Processor</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Risk Assessments</strong></td>
<td>Add privacy to annual risk assessment process Identify, calculate and treat risks</td>
</tr>
<tr>
<td><strong>Privacy Impact Assessments</strong></td>
<td>Implement PIAs where appropriate New or changes to existing processing activities</td>
</tr>
<tr>
<td><strong>Records of Processing</strong></td>
<td>Maintain records of processing activities Include details such as the type and purpose of processing</td>
</tr>
<tr>
<td><strong>Consent Management</strong></td>
<td>Ensure valid consent, where applicable Record consent details and maintain evidence</td>
</tr>
<tr>
<td><strong>Data Subject Rights</strong></td>
<td>Facilitate data subject rights Meet obligations and ensure transparency</td>
</tr>
<tr>
<td><strong>Vendor Management</strong></td>
<td>Maintain DPAs with third parties Assess and track processors and sub-processors</td>
</tr>
<tr>
<td><strong>Incident Response</strong></td>
<td>Identify, track and resolve personal data breaches Add privacy breaches to incident response plan</td>
</tr>
</tbody>
</table>
Benefits of ISO 27701 Certification

- Build trust and provide assurance
- Demonstrate compliance
- Promote continuous improvement
- Ensure flexibility and scalability
- Reduce risk
Program Preparation and Getting Certified
OUR CLIENTS
Build trust and assurance for clients that Accenture protects clients’ data and Accenture is in a position to help our clients do the same for their clients
Reduce formal compliance burden on clients (e.g., need to conduct audits)

OUR PEOPLE
Demonstrate to Accenture people our commitment to protecting personal data internally and externally

OUR REGULATORS
Offer strong evidence of compliance to applicable privacy requirements to which the Standards are mapped.

FUTURE
Potential use of certifications as a transfer mechanism
ACCENTURE DATA PRIVACY CERTIFICATIONS

A Global Standard for personal information management

Certifies the personal data controllership of Accenture’s enterprise

Future plans include certifying Accenture client engagement functions

Certifies Accenture client engagements that process EU data globally

A British Standard by BSI for personal information management

Controls correspond closely to ISO 27701 Standard

ISO 27701

BS 10012
A PRIVACY INFORMATION MANAGEMENT EXTENSION TO ISO/IEC 27001/27002 REQUIRES ISO 27001 CERTIFICATION

SETS STANDARDS FOR IMPLEMENTING AND MAINTAINING A PRIVACY INFORMATION MANAGEMENT SYSTEM (PIMS) FOR COMPLIANT PERSONAL DATA MANAGEMENT

CERTIFICATION OBTAINED 18 NOVEMBER 2019
Organizations that are ISO 27701 certified and looking to implement the requirements of ISO 27701 should consider taking the following steps:

- Perform a gap assessment of the existing Information Security Management System (ISMS) to the requirements of ISO 27701 and produce an action plan on how to address those gaps.
- Conduct a data mapping of the PII collected by the organization to understand the scope of PII collected and how it is used and shared with processors.
- Determine the organization’s role as a controller and/or processor based on internal or external factors that are relevant to its context, such as applicable privacy legislation, regulations, judicial decisions or contractual requirements (among others).
- Review and update privacy policies to ensure they contain the required information.
- Develop policies and procedures applicable to the organization’s role.
- Begin the planning and implementation of the privacy by design and default principles.
PIMS OPERATIONAL OVERVIEW

SCOPE OF PIMS

Personal data processing activities of global Client Data Protection (CDP) accounts across all Operating Groups and risk tiers, (“Client Service Business”), plus the personal data controllership activities of global Geographical Units and the supporting global Business Functions, (“Enterprise). See PIMS Operational Overview.

PIMS COMPONENTS AND CONTROLS IN RELATION TO ISO 27701

All controls of the ISO 27701 standard are applicable.

PIMS OBJECTIVES

- Establish commitment to continual improvement, including through certification and maintenance of an ISO 27701 certification
- Ensure awareness of and compliance with PIMS related requirements among CDP and Data Privacy personnel who support the PIMS
- Maintain green scorecard metrics against privacy controls in Company’s data management tool to validate effective implementation
- Conduct (at minimum) yearly PIMS Management Reviews to identify areas of improvement against PIMS performance

RESPONSIBILITIES UNDER THE GENERAL DATA PROTECTION REGULATION

Responsibilities are set out in individual job descriptions

KEY PIMS MANAGEMENT ROLES

- PIMS Steering Committee
- PIMS Executive Sponsor for Enterprise
- PIMS Executive Sponsor for Client Service Business
- PIMS Operational Oversight

PIMS MANAGEMENT REVIEW

The structure and process are described in the PIMS Management Review Process
**Steering Committee**

- Defines the scope the PIMS
- Ensures the PIMS is established, communicated, implemented, maintained and continually improved in accordance with the requirements of ISO 27701
- Participates in Steering Meetings

**Management Oversight**

- Participates in strategic planning and engages with the Steering Committee on PIMS priorities
- Leverages Steering Committee Forum to share risk information (i.e. from management reviews)

**Workstreams**

- Engages in tactical execution of PIMS priorities
- Directs and assists employees with day-to-day responsibilities for PIMS compliance and supports their contribution to the effectiveness of the PIMS

**Meeting & Update Frequency**

- Monthly

**Stakeholders**

- **Global Data Privacy** [names]
- **InfoSec** [names]
- **IS GRC** [names]
- **CDP (Client Service Business)** [names]
- **Data Privacy (Enterprise)** [names]

**Key Responsibilities**

- Defining the scope of the PIMS
- Ensuring the PIMS is established, communicated, implemented, maintained, and continually improved in accordance with the requirements of ISO 27701
- Participating in Steering Meetings

**Workstreams**

- **IS GRC** [names]
- **CDP (Client Service Business)** [names]
- **Data Privacy (Enterprise)** [names]
REQUIRED CENTRALIZED REVIEW AND GU LEVEL AUDITS IN IBERIA, INDIA, LATAM HSA, ASEAN AND NAM

AUDITS REQUIRED CLOSE PARTNERSHIP BETWEEN IS, DPISLS AND DATA PRIVACY WITH SUPPORT ACROSS CORPORATE FUNCTIONS

A COMPREHENSIVE ASSESSMENT OF ACCENTURE DATA PRIVACY PROCESSES AND CONTROLS

TRACKING SUGGESTIONS BY BSI AUDITORS IDENTIFIED DURING AUDITS AND TO BE ADDRESSED IN SHORT TERM
ASSESSMENT PROCESS

MANAGEMENT REVIEW

Completed July 26

DP and IS GRC
Review of the day-to-day PIMS effectiveness, at least annually or when a change occurs

GAP ANALYSIS WITH BSI

Completed Aug 29

DP and IS GRC
Review of ISO 27701 Standard and checklist of PIMS evidence

STAGE 1 ASSESSMENT

Completed Oct 11

DP and IS GRC
Review of PIMS documentation, recent Management Review report, and previous assessment action plans, if any

STAGE 2 ASSESSMENT

Completed Oct - Nov

DP and GU
Review of implementation of PIMS within selected GUs and Corp Functions that support the GUs

STAGE 2 DATA PRIVACY CENTRAL TOPICS

Completed Oct 29

DP
Review of centrally-managed Data Privacy functions, e.g. global risk assessment, training
ISO 27701

WHAT’S NEXT

- VALIDITY 3 (~2.5) YEARS
- REGULAR MANAGEMENT REVIEWS AND UPDATES TO OUR PIMS
- CONTINUOUS MONITORING MAINTENANCE AUDITS EACH YEAR
- EXPECTATION THAT ISO 27701 WILL AT SOME POINT BE ENDORSED BY EDPB UNDER ART. 42 GDPR
- BE READY FOR RE-CERTIFICATION IN 2022
ISO 27701 mapped to CIPL’s Accountability Framework
ISO 27701 mapped to CIPL’s Accountability Framework

PIMS-specific requirements related to ISO 27001:
- Context of the organization/Leadership/Planning/Support/Operation/Performance Evaluation Improvement

PIMS-specific requirements related to ISO 27002:
- Planning/Operation

PIMS-specific guidance related to ISO 27002:
- Asset Management

PIMS-specific reference control objectives and controls (PII Controllers):
- Planning /Operation

PIMS-specific reference control objectives and controls (PII Processors):
- Asset Management

PIMS-specific reference control objectives and controls (PII Processors):
- Privacy Impact Assessment

PII Sharing, transfer and disclosure:
- Records related to processing PII

PII sharing, transfer and disclosure:
- Records of transfer of PII

PII sharing, transfer and disclosure:
- Records of PII disclosure to third parties

Countries and international organizations to which PII can be transferred:
- Records of PII disclosure to third parties

PII Sharing, transfer and disclosure:
- Countries and international organizations to which PII can be transferred

Records of transfer of PII:
- Records of PII disclosure to third parties

PII Sharing, transfer and disclosure:
- Records related to processing PII

PII Sharing, transfer and disclosure:
- Records of PII disclosure to third parties

PII Sharing, transfer and disclosure:
- Identifies basis for PII transfer between jurisdictions/Countries and international organizations to which PII can be transferred

PII Sharing, transfer and disclosure:
- Records of transfer of PII

PII Sharing, transfer and disclosure:
- Records of PII disclosure to third parties

PII Sharing, transfer and disclosure:
- Customer agreement/Records related to processing PII

PII Sharing, transfer and disclosure:
- Identify and document purpose/Identify lawful basis/Obtain and record consent/Privacy impact assessment

PII Sharing, transfer and disclosure:
- Identify and document purpose/Identify lawful basis/Obtain and record consent/Privacy impact assessment

PII Sharing, transfer and disclosure:
- Identify and document purpose/Identify lawful basis/Obtain and record consent/Privacy impact assessment

PII Sharing, transfer and disclosure:
- Identify and document purpose/Identify lawful basis/Obtain and record consent/Privacy impact assessment

PII Sharing, transfer and disclosure:
- Identify and document purpose/Identify lawful basis/Obtain and record consent/Privacy impact assessment
Questions?