IAPP **ASIA FORUM 2026**

Privacy | AI governance | Cybersecurity law

Training 21 July

Conference 22-23 July | SINGAPORE

#IAPPForum26

FROM ZERO TO HERO

Building a Risk-based Privacy Program on a Budget

WELCOME AND INTRODUCTIONS

Angelo Tiglao, AIGP, CIPP/E, CIPM, CIPT, FIP

Associate, Intellectual Property, Data and Technology, Quisumbing Torres

Pia Agatep

Privacy and Data Protection Counsel

Aica Palce-Reago, CIPP/E, CIPM, FIP

Senior Legal Counsel for Data Protection & Privacy, SAP

Bianca Villarama, JD, AIGP, CIPM, CIPT

Director, Regulatory & Privacy, Tala

FROM ZERO TO HERO

Building a Risk-based Privacy Program on a Budget

FROM ZERO TO HERO

Building a Risk-based Privacy Program on a Budget

The Jurisdictional Maze

🧯 Managing Endless Fires

Privacy professionals in Asia-Pacific face disjointed, overlapping, and constantly changing regulations.

- **Blanket audits:** Trying to secure everything at once burns finite team resources instantly.
- **Reactionary posture:** Fighting localized compliance requirements on a purely transactional basis.
- **The cost trap:** Treating compliance as an expensive, unyielding administrative block.

The Risk-Based Paradigm

Focus Where Exposure is Highest

By pivoting to a risk-based framework, privacy leaders can bypass blanket compliance overhead and achieve rapid strategic victories.

- **High-exposure priority:** Budget and assets are exclusively targeted at critical data flows.
- **Strategic alignment:** Translates abstract legislation into practical, localized data handling guardrails
- **Empowered growth:** Elevates the legal team from a cost-center bottleneck into a trusted scaling partner.

The Resourceful Privacy Leader

Maximizing Free and Pre-paid Resources

INTERNAL TOOLS

Productivity & Workspace Tools

- Built-in labeling/RBAC/compliance features
- Spreadsheets for privacy and TPR assessments
- Forms for intake processes

Existing Intranet & IT Systems

Unearth pre-configured internal knowledge bases, communication portals, and technical infrastructure.

EXTERNAL RESOURCES

Regulators & Authorities

Official templates, published guidance, and standard compliance frameworks

External Legal Counsel / Consultants

Retainer advisory hours, legal update newsletters, and expert reference materials

Industry & Peer Networks

Shared best practices, consulting communities

AI TOOLS

Generative AI Use Cases

First-pass assessments, summarize multi-jurisdiction regulations or generate employee awareness content.

⚠️ **Guardrails**

Stay within the organization's approved guidelines for the use of enterprise AI tools.

Risk-Based Approach

HIGH-RISK PIPELINES

- **Understanding the Organization's Risk Profile and Risk Appetite**
- **Mapping the 3 Critical Data Pipelines, e.g.,**
  - **Customer Onboarding:** High-volume entry point; mapping of personal/sensitive data
  - **Payment Processing:** Critical financial data; varying levels of identifiability
  - **Third-Party Marketing Tools:** External trackers creating compliance exposure

STRATEGIC PRIORITIZATION

- **Must-Have vs. Nice-to-Have Measures**
  - **Must-Have:** Core security controls to reduce the highest-impact industry risks
  - **Nice-to-Have:** Secondary operational enhancements to be built/implemented after high-impact vulnerabilities are addressed

Advocating for Budget and Support

THE AUTOMATION ARGUMENT

Free/available resources saved significant manual effort during the initial launch, but easily hit limits for scaling.

- **Unlock High-Value Work:** A budget injection for automation frees up valuable bandwidth.
- **From Support to Strategy:** Transition key stakeholders from daily admin to strategic, value-creating initiatives.

BUDGET CO-OWNERSHIP

Privacy & Compliance

20%

Core Privacy Budget

Mandatory regulatory reporting, direct compliance requirements, and fundamental operational program oversight

Data Quality & BI

40%

Data Engineering Support

Structured labeling and precise data classification schemas that directly optimize downstream analytics pipelines

Cyber-Risk Security

40%

Infosec Budget

Minimized data exposure footprint, neutralizing system vulnerabilities and attack surface areas

Incident Management

Building Blocks of Incident Readiness

TEMPLATES PREPARED IN ADVANCE

- Breach / incident triage intake form
- Regulator notification template with jurisdiction-specific fields
- Templates kept current on a regular review cycle, so the version you reach for is always the latest approved one.
- Templates are stored where every responder can find them quickly.

TRIAGE AND ESCALATION

- Every incident type has its own path. Triage routes it to the specialist team equipped to act on it quickly.
- Triage responsibility is staffed across regions and time zones, so an incident raised outside standard hours still gets picked up quickly.
- If an incident is heading toward a regulator or individual notification, local management is informed immediately.

DETECTION STARTS ON THE FRONT LINE

- Mandatory trainings so employees know what qualifies as reportable and how time-critical it is.
- Detection does not depend solely on the privacy team noticing.
- Every employee is a potential first responder.
- Pair training with a simple, well-publicized channel, so people know exactly where to flag something.

Cost-effective Compliance while Navigating Overlapping Global and Regional Regulations

The Multi-Jurisdictional Dilemma

Different National Regimes

MNCs simultaneously traverse different, overlapping laws across APAC, the US, UK, and EU. Keeping track of contrasting regional definitions, localization demands, and transfer rules wastes vital overhead.

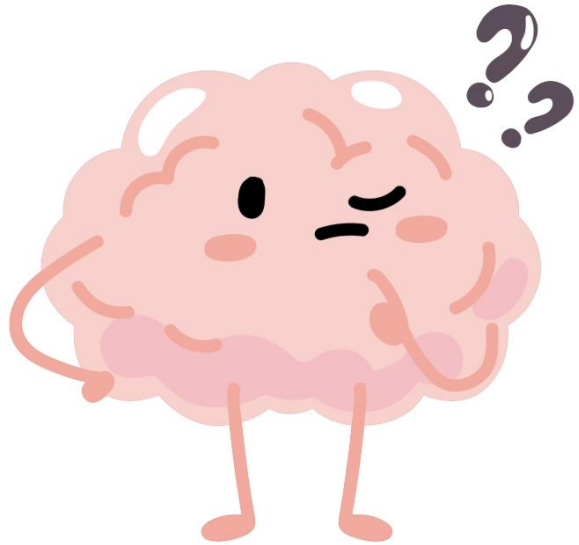
Escalating Audit Exposure

Enforcement is shifting rapidly. With cumulative GDPR fines exceeding €7.1 Billion and escalating local updates, regulators penalize programs that are clearly "tick box exercises." Good faith must be documented.

Minimum Viable Defensibility

The trap of perfect coverage leads directly to operational burnout. MNCs must replace legal abstraction with targeted workflows, utilizing unified standards to clear several regional hurdles at once.

BEFORE YOU SPEND, ASK THESE FIRST.



1 Where are we actually processing personal data?

- Not where you might expand, but where are you active now?
- A number of data protection laws have extraterritorial reach. Presence is not required to trigger an obligation.

2 **Which regulators are actively enforcing and what do they target first?**

- Which extraterritorial laws (GDPR, CCPA, DPDPA) are triggered?
- Are we exposed to hard mandates (local reps, localization) risking operational shutdowns?
- Knowing what regulators look for and not just what the law says determines where to focus limited resources.

3 **Are we building fifteen programs or one?**

- Managing a separate compliance program per jurisdiction is unsustainable.
- Identify the strictest applicable global standard and build to that. Let everything else fall into compliance beneath it.

4 **Do our people's roles create structural conflicts?**

- Do double-hatted internal champions create immediate audit vulnerabilities?
- Are the people accountable for auditing workflows the exact same builders creating them?
- If the person accountable for data governance is also the sole creator and sole auditor of processing activities, that is a compliance vulnerability regardless of their competence.

5 **What compliance infrastructure do we already own?**

- IT asset registers, vendor contracts, ticketing systems, and internal communication tools are all latent compliance assets. The question is whether they are being used that way.

Phase A: Set Your Strategic Foundation

The "High Water Mark"

Identify the strictest applicable global standard and build your internal processes to meet the strictest applicable global standard. Satisfying the highest threshold helps ensure that lower regional targets fall into place automatically.

Build once at the ceiling. Adjust locally at the margins.

Double-Hat Responsibility Matrix

When staff must multi-task, document non-conflicting operational borders explicitly. Build a clean, single-page RACI chart assigning non-conflicting privacy responsibilities across legal, IT, HR, and procurement.

Ensure that the person who creates data-processing activities is not the sole person auditing them.

Evaluate an Outsourced or Fractional DPO

Where hiring a dedicated full-time data protection officer is unviable, leverage a fractional or outsourced DPO model. Outsource when allowed, but keep a clear internal accountability through a designated staff escalation champion who will feed context to the external provider and ensure advice is operationalized.

Phase B: Embed Privacy Before Problems Arise

Privacy by Design is not just good practice. It is a force multiplier: every process built with privacy in mind is one fewer incident, one fewer remediation cost, one fewer regulator conversation.

Make Privacy a Gate in the Dev Pipeline

Embed a mandatory privacy checkpoint in Jira/GitHub release templates before any new feature ships

For ML/AI features, add a dropdown: 'Does this use automated logic to categorize, approve, or deny a user?'

Filter monthly free algorithmic risk registry

Default to Data Minimization and Privacy Protection Settings

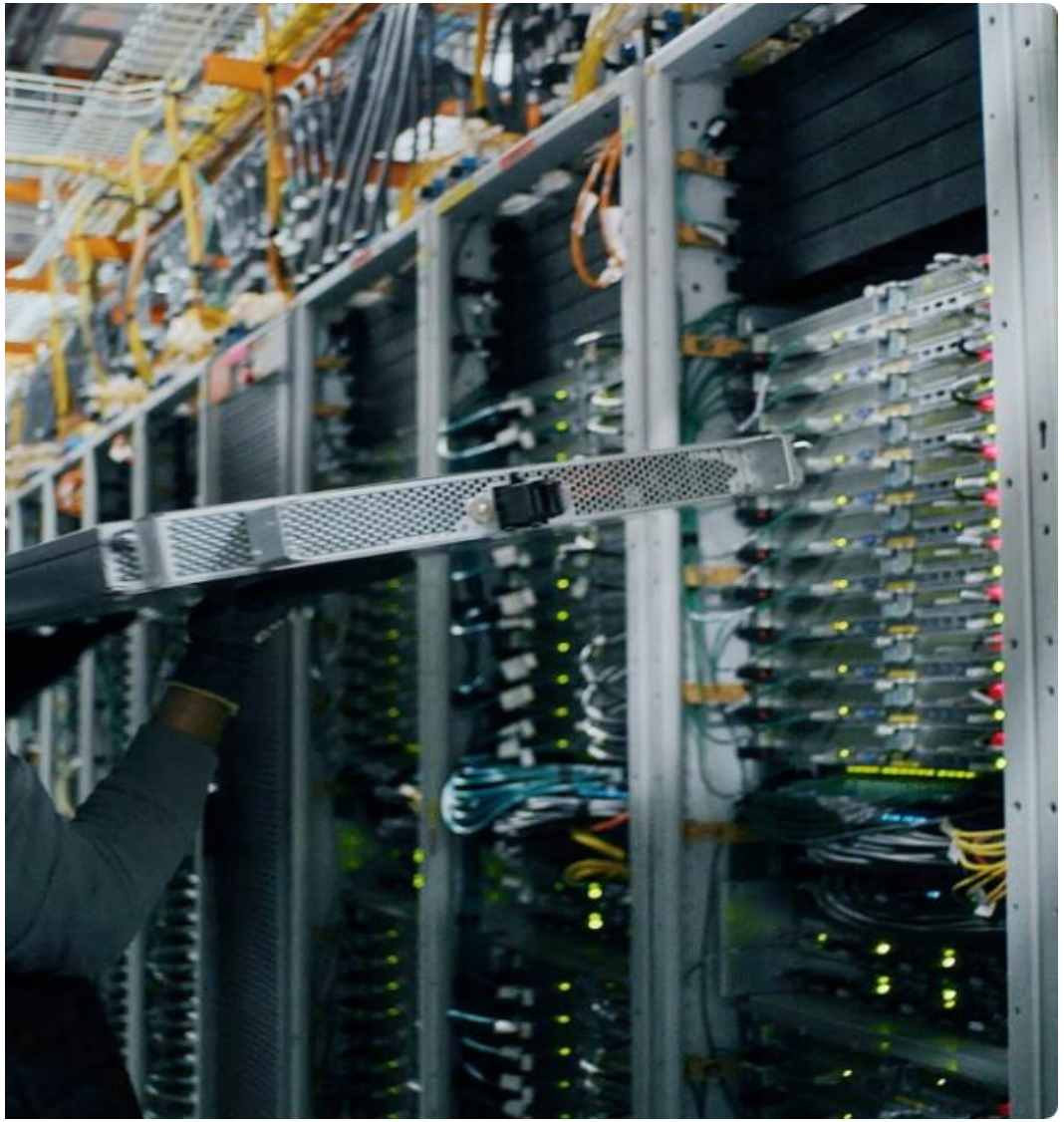
Configure new products so optional data collection is off by default, marketing tracking requires opt-in, and retention periods are set at the point of system design.

Work with DevOps to run automated deletion/anonymization scripts on cold data every 90 days.

Conduct Lightweight Privacy Impact Assessments (DPIAs)

You can use the free one-page screening template from the UK ICO or Singapore PDPC.

If the answer to all screening questions is 'No' the template itself is the record of assessment. If 'Yes', document a deliberate decision before launch.



Phase C: Build Your Compliance Infrastructure from What You Already Have

Piggyback Data Mapping onto Existing Assets

Do not purchase complex discovery tools. Add data classification, access privileges, and server location columns to existing ISO 27001 or SOC 2 asset logs to establish a global map with zero overhead.

Compile Your "Defensibility Binder" Before You Need It

Keep a centralized folder of current transfer mechanisms, training logs, vendor DPAs, and regulator self-assessment answers to proactively signal good-faith governance.

Phase D: Operationalize Transactions & Response

Master Global DPA Annex

Deploy a master Global Data Protection Annex compiling unedited transfer templates (EU SCCs for Western flows, ASEAN MCCs for Southeast Asian flows) to attach to standard vendor agreements.

Sync Incident Response

Sync incident response to strict statutory reporting timelines. Establish a dedicated triage channel on Slack or Teams with a pinned 3-question intake form to automate alerts the moment a breach is noticed.

Enforce Data Minimization

Partner with DevOps to deploy automated deletion/anonymization scripts targeting cold server logs, expired marketing lists, and inactive user profiles to shrink liabilities and cloud storage costs.

THE BOTTOM LINE

Regulators don't expect a million-dollar software stack.

They expect to see:

- A documented data inventory
- A clear internal accountability structure
- Evidence of deliberate, risk-based prioritization
- Proof you acted — not proof you acted perfectly

Budget-conscious compliance is entirely achievable when privacy stops being a standalone legal project and becomes an operational filter applied to the workflows our organizations are already running.

Fireside Chat

Q&A

RESOURCE LIST

Helpful Resources & Links

- PDPC Notice Generator
- NPC (PH) Guide for Creating a Privacy Manual
- AI Policy Template (Australia National AI Centre)
- Sample Clause for Data Transfers to APEC and Global CBPR and PRP Certified Organizations
- Documentation template for controllers
- Documentation template for processors
- ASEAN Model Contractual Clauses and EU Standard Contractual Clauses

Speakers' Contact Info

Angelo Tiglao
linkedin.com/in/angelotiglao

Pia Agatep
linkedin.com/in/piaaagatep

Aica Palce-Reago
linkedin.com/in/aicapalce

Bianca Villarama
linkedin.com/in/biancavillarama

How Did Things Go?
(We Really Want To Know)

Did you enjoy this session? Is there any way we could make it better? Let us know by filling out a speaker evaluation.

1. Open the IAPP Events app.
2. Select **IAPP Forum 2026**.
3. Tap "Schedule" on the bottom navigation bar.
4. Find this session. Click "Rate this Session" within the description.
5. Once you've answered all three questions, tap "Done".

Thank you!