Generated by Microsoft Designer.

Manage Supplier Risk, Shorten Your Procurement Cycle and Be a Hero to All!

WELCOME AND INTRODUCTIONS

Peggy Eisenhauer, CIPP/US
Founder, Privacy & Information Management Services

Jonathan Fox, CIPP/US, CIPM
Director, Strategy and Planning, Cisco

John Gevertz, Of Counsel, DLA Piper, former CPO Visa and ADP

PROGRAM OUTLINE

1. Supplier Risk Management

2. Data Processing Agreements (and how to negotiate them)

3. Additional Requirements and Special Situations

4. Your questions!

RESOURCE LIST

- Supplier Information Sheet
- PIMS Template Data Processing Agreement – *Feb 2024 Annotated Final*

Supplier Risk Management

Privacy laws regulate supplier relationships

- US Federal laws (such as GLBA and HIPAA) and state laws require companies to manage their processors and to have appropriate contracts with data processors – CCPA Regs have specific contract terms in § 7051
- International laws, such as the GDPR, have specific rules for suppliers, including required contract terms – see GDPR Art 28.

Summary of the Legal Requirements:

Companies must (1) take reasonable steps to select suppliers that can provide appropriate safeguards for the personal information, and (2) contractually require the suppliers to implement and maintain such safeguards:

- Assess the specific risks related to the services provided
- Conduct appropriate due diligence on the supplier
- Contractually require the supplier to limit use of data as needed to perform the services and to maintain appropriate safeguards – *include using required contract terms in some cases*
- Oversee the supplier's activities as reasonably needed to assure compliance

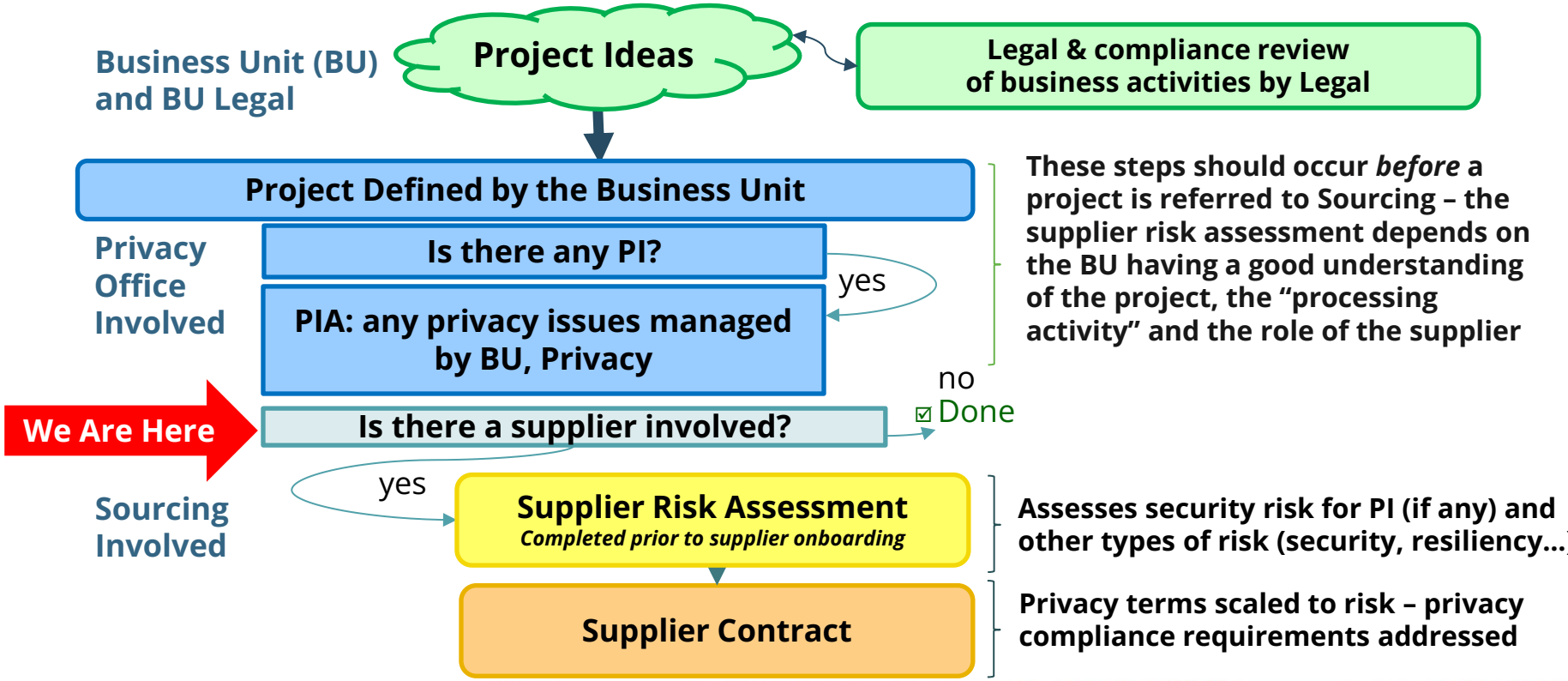
Supplier Due Diligence

- Effective risk assessment requires collaboration between the business and the sourcing, security and privacy functions.
- Risks of the processing activity should be assessed (and mitigated) before the supplier is engaged
- This requires the business to clearly explain *what* the supplier will be engaged to do, including describing the data & data flows accurately
- *"Privacy due diligence" is in addition to other types of risks that you manage: commercial risks (competence, resiliency), financial risks (creditworthiness, stability), ESG, geopolitical…*

Not an Effective Process

La Brea Tar Pits Photograph by Michael Long/science Photo Library

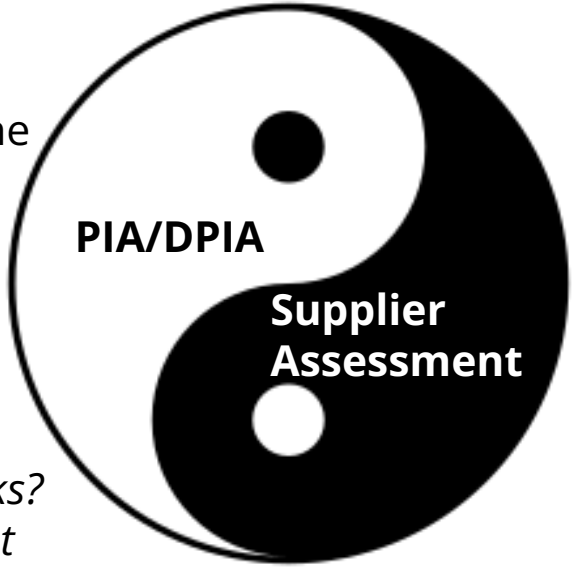
Privacy Risk Management – An Effective Process



PIAs vs. Supplier Privacy Risk Assessments

Assesses the risks of the *processing activity*
- employee screening
- running a compliance hotline

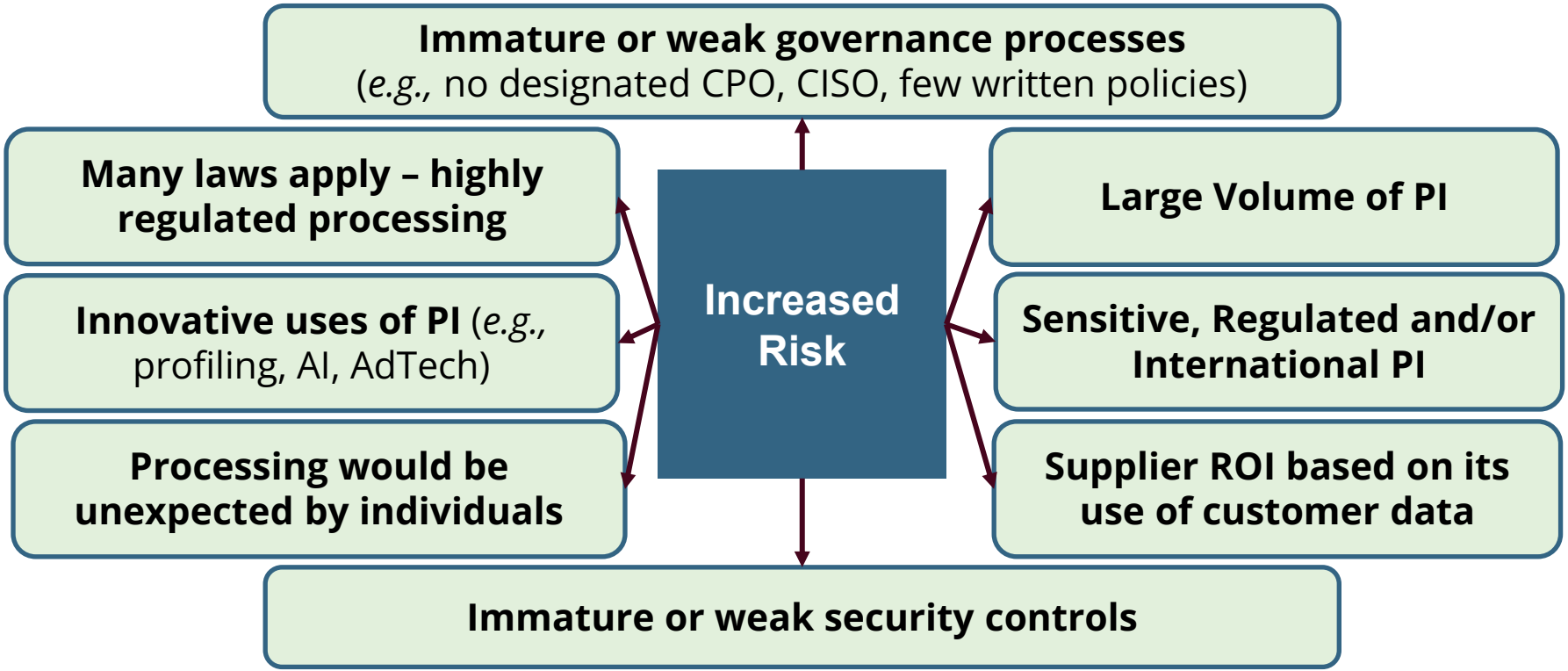
- *Is it legal?*
- *Do individuals expect it?*
- *Do we need consent?*
- *Does it put people at risk?*
- *Is it "high risk"?*
- *How do we mitigate the risks?*
- *Are the benefits greater that the risks?*



Assesses risks of the *company* doing the processing for us
- HireRight
- Navex

- *Can they meet our security requirements?*
- *Will they commit to only using the data to provide services to us?*
- *Will they respond appropriately if they have a security breach?*

Consider different types of risks



Specific Risks for “Privacy” to Consider

- Risks associated with the “processing activity” – *these should have assessed by a PIA, but that doesn’t always happen, esp. if the supplier is selling you a new service*
- Risks associated with potential breaches & loss of data – *even if there’s no a malicious action, the unavailability of data may be a breach under GDPR*
- Risks associated with emerging technologies – *what type of GAI is being used? Will your data be used to train the system?*
- Supplier-induced risks – *secondary use of data, DSR response complexity, data retention*
- Understand the handshake with your CISO for security due diligence, risk assessment of downstream processors (subprocessors) and with sourcing for commercial risks

Good Supplier Governance is a Benefit

- Mapping your entity's Total Available Market (TAM) of Data
- Feeding your ROPA
- Building a foundation for accountable transparency
- Improving efficiency of incident response
- Driving collaboration and process alignment
- Vendor eco-system improvement
- Sleep

What you need to know for the contract phase

- What functions are being outsourced? What PI is being processed? Does the processing involve novel technologies, such as use of generative AI? – *the contract should address nuances of the relationship based on the services provided.*
- Do the data include regulated data (such as PHI subject to HIPAA or student data)? – *if so, the contract needs to include appropriate terms (e.g., BAA)*
- Will the supplier collect personal information directly from individuals for us? – d *verify that an appropriate privacy notice will be provided to the individuals*
- Are there any data transfers? – *ensure that subprocessors and cross-border transfers are properly documented*

Data Processing Agreements

If there's not much PI, do we really need a DPA?

Yes.

- Many laws require companies to have contracts with their processors.
- Having a contract demonstrates your own commitment to complying with privacy laws.
- It's the easiest (and a generally non-objectionable) way to mitigate risk.

The secret is to use terms that are as balanced and business-friendly as possible.

The DPA should set expectations

We expect our suppliers to:

- Comply with the laws that are applicable to them
- Only use our PI to provide the services *and for other pre-approved internal uses*
- Maintain appropriate security controls
- Manage risks related to subprocessors and their own cross-border transfers
- Tell us promptly of any security incidents
- Delete our information when its no longer needed to provide services
- Accept appropriate oversight from us and our regulators

DPA Basic Terms

- Applies to PI processed “for the customer” – does not apply to PI collected by the supplier for its own purposes (such as data pertaining to system users)
- Only use, disclose the PI to provide services and for “internal business purposes
- Both parties agree to comply with applicable privacy laws
- Specific compliance terms “to the extent applicable” (GDPR, CCPA, HIPAA, PCI DSS…)
- Secure the PI using appropriate safeguards
- General limits on data transfers, subprocessors
- Provide reasonable support for PIA/DPIAs, DSR requests…
- Accept audits
- Return or delete the PI at the end of the term

All of these things are required by law

Supplier Pain Points – Reasonable Requests

- Liability for things in our control
  - *processing based on our instructions*
  - *our data is not appropriately permissioned*
- Unreasonable or unmanageable obligations
  - *notify of suspected security events immediately*
- Overly disruptive obligations
  - *overly broad audit rights*
- Unlimited liability

These are reasonable objections! Don't ask for these things!

Supplier Pain Points – Find Common Ground

You have to have what you have to have, but consider specific objections.

- Liability for things they have to control
  - *subprocessor activity, internal negligence*
- Difficult (but legally-required) obligations
  - *notify of security incidents without undue delay*
  - *notify Acme of subprocessors, transfers*
- Disruptive (but legally-required) obligations
  - *reasonable audit rights*
  - *delete data upon termination*

Consider the value of the contract; it may be okay to assume some liability.

What can they commit to? E.g., notify of "confirmed" breaches?

Tie provisions to their actual processes. E.g., reflect that audit rights may be limited if data are hosted elsewhere.

Problematic Supplier Positions

- Unwillingness to accept any liability
  - *but consider value of contract to the supplier*
- Unwillingness to accept limits on their own use of your data
  - *but consider if they are really a "data processor"*
- Inability to meet required security standards
  - *but consider if there are compensating controls*

Have a documented path for escalation of risk.

Indemnification & Liability

- Many DPA templates include liability terms and indemnification. These almost always burden the negations!

- The PIMS Template DPA requires the supplier to bear the costs of any security incidents that are caused by its negligence or breach of the contract, **but it does not contain any general indemnification provisions**.

- The better path is negotiate indemnification and liability cap clauses only once, in the main contract, as may be appropriate for the relationship overall, given all of the factors (such as pricing/value of the contract, *etc.*).

Additional Requirements & Special Situations

About “applicable laws”…

Suppliers don’t always know what laws are applicable to them.

- For example, a US-based supplier may not be familiar with the GDPR requirements, but we must include these if the supplier might process EU/UK PI
- Smaller suppliers may not be subject to new US laws, such as My Health My Data…

Everyone has to work together to make sure that the requirements are understood!

Suppliers who are not “data processors”

- MOST suppliers are Data Processors… they are only meant to use the PI to provide the services
- But some third parties will need to use the information for their own purposes, subject to other laws:
  - employee benefits providers, such as health insurance companies, healthcare providers, financial institutions
  - Background screening companies
  - Fraud and security consortia
  - Certain telecommunications providers
  - Law firms, accounting firms

Document the basis for the disclosure (*e.g.*, consent) – contract provides that each party complies with laws applicable to it as a *controller*.

Data Transfer Considerations

Some privacy laws restrict data transfers, including:

- Transfers to other COMPANIES, even within the same country
- Transfers to other COUNTRIES, even within the same company

“Transfer” means both the physical movement of data to a recipient AND virtual movement that occurs when the data are remotely accessed by a recipient.

Data Transfer Considerations

Most laws simply require that we use contractual controls to assure the same level of protection for personal information after the transfer. BUT:

- EEA, Swiss and UK laws require that transfers of PI to “non-adequate” countries (such as the US) be authorized using an approved mechanism
  - Standard Contractual Clauses, aka “model contracts” or SCCs
  - Binding Corporate Rules (BCRs)
  - Data Privacy Framework

- Argentina, China, New Zealand and other countries also require model contracts or BCRs.

Data Transfer Considerations

- Suppliers should indicate if there are any cross-border data transfers. If so:
  - Supplier can indicate what mechanism(s) it uses to authorize the transfers. *When in doubt, use the SCCs*
  - The SCCs do not get negotiated! The are “model” terms published by the regulatory authorities.
  - The Supplier completes the Annexes to the SCCs. Many suppliers have standard annexes that can just provide you.
- If there are transfers to other companies, the Supplier can list the subprocessors.

Questions about Anything (Supplier Related)

Generated by Microsoft Designer.

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 Cvent Events app.
2. Enter **IAPP PSR24** (case and space sensitive) in search bar.
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”.