May 26, 2021

Sharing Data and Managing Third Parties Across the Worldly Divide

Privacy+ Security Forum

Speakers

Debra Bromson

Associate General Counsel at AAA Club Alliance Inc.

K Royal

Associate General Counsel at TrustArc

Maggie Gloeckle

Associate General Counsel, Head of Global Privacy at A+E Networks

Wayne Unger

Founding Attorney, The Unger Firm LLC
Visiting Assistant Professor of Law, Gonzaga University School of Law*

*Starting Fall 2021

What we will Cover

- The “Why?” Behind the Program
- The Vendor Management Program
  - Basic Programmatic Elements
  - Sectoral Nuance & Complexities
- Improving a Program in Flight
  - Maturing your program to where you want to be
- Tips
- Resources

Why? (and why now?)

- Disruptions
- Public awareness
- High profile data breaches
- Law & regulatory developments
- Increased scrutiny
- COVID-19

This never happens, right?

Today

K Royal 3:25 PM
Hey Wayne

Wayne Unger 3:25 PM
Hey

K Royal 3:25 PM
So we just got an email from one of our marketing providers

I am hoping I can send it to you

Wayne Unger 3:25 PM
Okay

K Royal 3:25 PM
I am sure it is fine

Wayne Unger 3:26 PM
What do you need me to do with it?

K Royal 3:26 PM
Well, they said that they had a possible incident, but they don't think it is a breach, but they want us to confirm that they told us and we are okay with it

Wayne Unger 3:26 PM
Ok

Who is it from?

K Royal 3:28 PM
All marketing everywhere - out of the Ukraine

Maggie G 3:28 PM
which company is this for

Wayne Unger 3:28 PM
Never heard of them

K Royal 3:28 PM
they integrate with Salesforce and Netsuite to drive our targeted gaming system

Wayne Unger 3:28 PM
We use them?

Doesn't ring a bell

K Royal 3:29 PM
But you can still sign off, right? They said it was only names, and IP addresses, the games they use, and the messaging in the games,

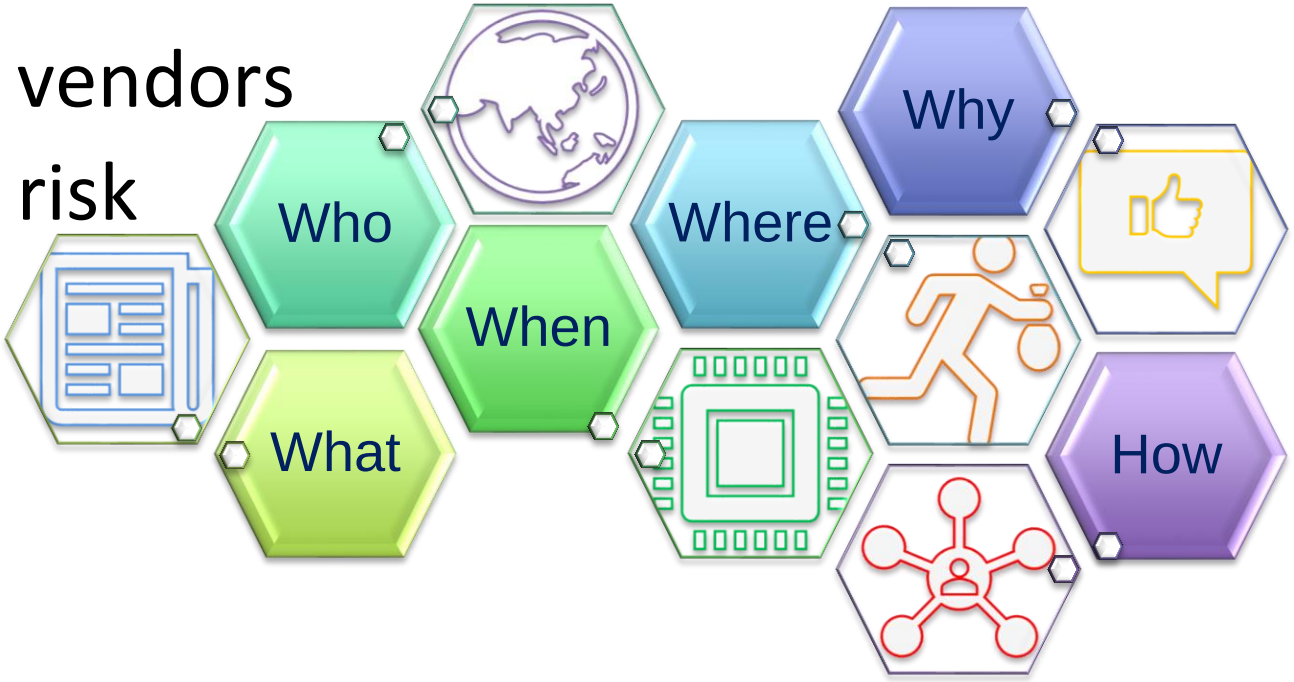
oh and purchases

Basic Programmatic Elements

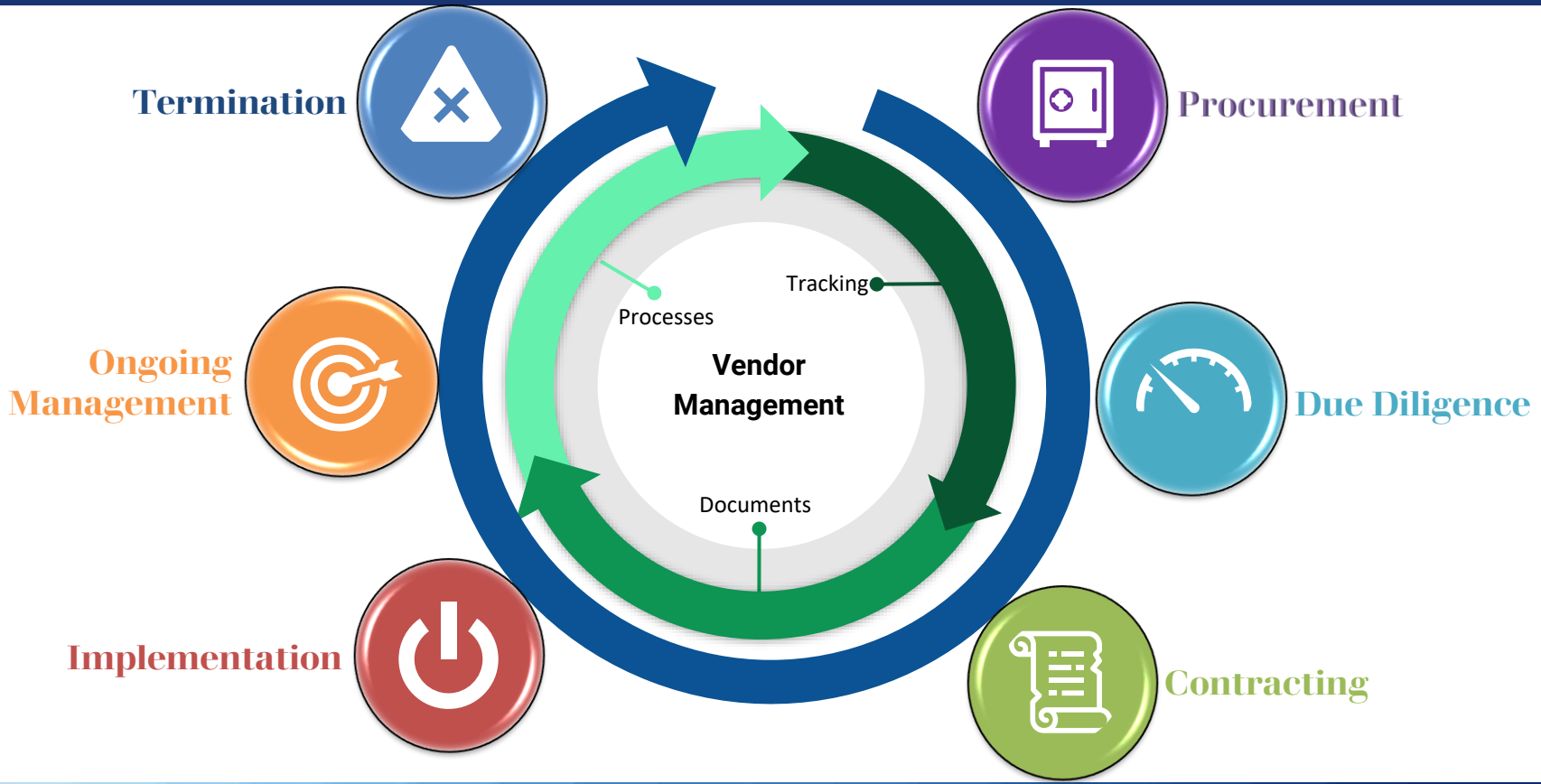
Approach, Lifecycle, Sectoral Nuances, & Complexities

Approach

- Know your data
- Know your vendors
- Know your risk



Vendor LifeCycle



Procurement

- Starting point, even if informal
  - MNDA / NDA
  - RFP / RFI - include key elements for privacy and security
- If procurement has a form, add in key elements to assess
  - What types of information they will receive / or you will share?
    - [need a data classification]
    - this includes employee log-on information
  - How do they receive or access data?
  - Where do they process data (storage and access, too)
  - How do they process data (on prem, cloud, data feed, etc.)
- If there is no procurement or they don't have a form, identify if there is a process starting point

Initial Due Diligence

- Conduct risk-based due diligence
  - Classify vendors by risk for your company
  - Risk assessment for “red flags” and risk factors
  - Review publicly available information, e.g., website, SEC filings
- Risk Tolerance (legal, compliance) - company culture
- Vendor Tracking - spend threshold vs. data classification
- Third parties of vendors (subprocessors) and the type of services needed

Enforcement

- GDPR / US / Other jurisdictions are taking action against vendors
  However, cannot waive negligence

Contracting

- Who – you
- What – the MSA and the associated addenda
- When – set triggers and parameters
- Where – identify locations that are approve, what actions to take, and which ones to alert on
- Why – need visibility, legal, compliance, etc.
- How – contract processes, auto alerts, business team

- Extras – DPA, SCC, BAA, Code of Conduct, Security requirements
- Additional Safeguards under Schrems II

Implementation / Onboarding

- Who – business owners
- What – are they accessing? What data? What systems? What policies?
  - Track non-standard contract terms, did you put in requirements?
- When – before they start
- Where – confirm locations
- Why – regulators, customers, end users may ask. You need to be able to answer
- How – connections around company, tracking systems, checklists

Ongoing Management

- Who – business owners, procurement, accounts payable, contracts
- What – confirm all points you are tracking or captured, update information, re-assess (risk-based on data, location, processes)
- When – annually on renewal or less based on risk
- Where – confirm locations of processing, subprocessors, etc.
- Why – risk changes, use changes – they may have increased services or scope
- How – develop processes, tracking points, relationships

Termination

- Who – business owners (executives), accounts payable
- What – data and access
- When – on termination, if contract date, confirm date to cancel by
  - If for cause, have that relationship with business owner
- Where – are there copies of data anywhere?
- Why – protect the data
- How – relationships, processes, checklists
  - If cannot delete, identify why and for how long
  - Certification of destruction
  - Backups – be practical

Sectoral Nuances

- Healthcare 
- Financial
- Insurance 
- Education 
- Minors
- Biometrics 

Complexities

- Be on the same page, literally
  - Define terms, e.g., “Sensitive” “Confidential” “Incident” and avoid circular terms
- Local law
- Coordination – individual rights, law enforcement requests, etc.
- Changes in law, delays in enforcement, temporary arrangements
- Culture and expectations
- Multiple contract reiterations, with amendments, renewals, cancellations, addenda, etc.
- Mergers and acquisitions
- Force majeure

Building a Program

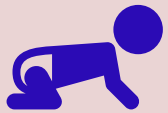
Starter Package, In Flight, Tips

Starter Package - Program

Know your data and activities	Where is your data and where does it flow? Who and what has access?
Sponsors and stakeholders	Identify supporters and detractors (and the influence scope of both)
Risk landscape	Need to know limits and parameters; internally and externally
Compliance landscape	Need to know what applies and scope

The Plan – Back to Basics

1



Develop Strategy

2

Establish Governance

3

Train and Implement

4

Assess and Improve

The Things You Need

Contracts

Clauses

Identify critical elements

DPA / SCC

Addenda

Triggers for review

Policies

Third party interactions

Data retention and destruction

Incident response

Data classification & handling

Training

DR / BCP

(of course, Privacy, Security)

Processes & Tools

- ❑ Dataflows & inventory
- ❑ DPIAs / PIAs
- ❑ Privacy / Security assessments
- ❑ Framework – GDPR? ISO27001?
- ❑ Tracking (contracts, parties, laws)
- ❑ Cross-border transfers – identify when occurring, know what is legal
- ❑ Compliance calendar
- ❑ Notifications (subprocessors, etc.) - email (notice provisions in contract)

In Flight

Assess your program

- Do you have the elements in place that are fundamental?
- What are your pain points?
- If a customer came to audit… how would you react?

Common elements (that we can all improve)

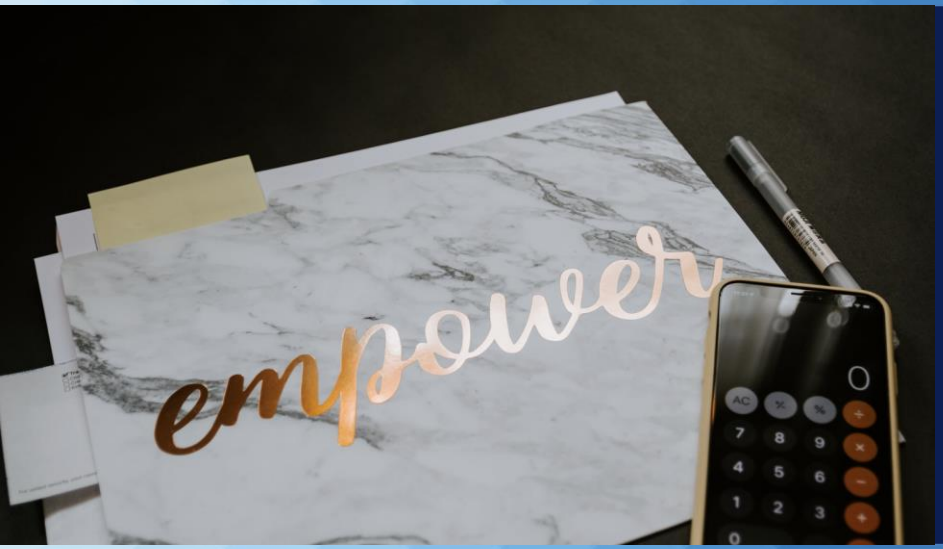
- Identify who and how to re-assess based on risk
- Track things you need to know (including staying up to date)
- Dataflows and inventory
- Employee understanding of why it matters (free is dangerous)
- Resources – manual vs. tools

Tips

- Responsibility without authority is awful
- Use a framework
- Partner with internal audit and security
- Be practical and reasonable
- Preach privacy, often, in many ways, use pictures and examples
- Reward twice as much as you correct
- Try to make compliance fun
- Separate policies from procedures
- Move towards certification
- Build internal friendships
- Learn to influence and identify detractors

Privacy+ Security Forum

Questions



Resources

Privacy+ Security Forum

Photo by Kelly Sikkema on Unsplash

Resources

- **Privacy Law's False Promise, Washington Law Review**
  (discussing how current privacy laws lead to symbolic compliance and not actual privacy)
  https://openscholarship.wustl.edu/cgi/viewcontent.cgi?article=6386&context=law_lawreview
- ***Katz* and COVID-19: How a Pandemic Changed the Reasonable Expectation of Privacy, Hastings Science & Technology Law Journal**
  (discussing health surveillance technologies, data supply chains, and how the pandemic changed privacy expectations)
  https://dx.doi.org/10.2139/ssrn.3692652
- **Privacy & Market Concentration: Intended & Unintended Consequences of the GDPR**
  (suggesting that vendors are more likely to drop smaller vendors—leading to an increase in market concentration among web technology vendors)
  https://www.ftc.gov/system/files/documents/public_events/1548288/privacycon-2020-garrett_johnson.pdf
- ***AMG Capital Management, LLC v. Federal Trade Commission***
  A recent United States Supreme Court decision that provided "Section 13(b) [of the FTC Act] does not authorize the [FTC] to seek, or a court to award, equitable monetary relief such as restitution or disgorgement."
  https://www.supremecourt.gov/opinions/20pdf/19-508_l6gn.pdf
- **Measuring and Protecting Privacy in the Always-On Era, Berkeley Technology Law Journal**
  (discussing legal and computational methods that could be used by IoT service providers to optimally balance the tradeoff between data utility and privacy).
  https://btlj.org/data/articles2020/35_1/05_Haber_FinalFormat_WEB.pdf

Resources

- **Verifiable Vendor Management: 4 Tips to Avoid Risk**
  https://www.accdocket.com/articles/verifiable-vendor-management-4-tips-to-avoid-risk.cfm
- **Your Vendor Your Risk- By Maggie Gloeckle and K Royal | 2019-Oct-01**
  https://www.accdocket.com/articles/resource.cfm?show=1503009
- **NIST: Privacy Framework** https://www.nist.gov/privacy-framework/privacy-framework
- **Third Party Vendor Management Means Managing Your Own Risk** (series) https://iapp.org/news/a/third-party-vendor-management-means-managing-your-own-risk/
- **Third-Party Relationships: Frequently Asked Questions to Supplement OCC Bulletin 2013-29**
  https://www.occ.gov/news-issuances/bulletins/2020/bulletin-2020-10.html
- **Creating a Strategic Roadmap for Vendor Management**
  https://www.gartner.com/smarterwithgartner/creating-a-strategic-roadmap-for-vendor-management/
- **3 Steps to Improve Strategic Vendor Management**
  https://www.gartner.com/smarterwithgartner/3-steps-to-improve-strategic-vendor-management/
- **Outsourcing Technology Services**
  https://ithandbook.ffiec.gov/it-booklets/outsourcing-technology-services.aspx
- **Privacy Now: Predicting 2021's Legal Tech Trends (ACC Docket, K Royal)**
  https://www.accdocket.com/node/538

Questions + Contact

Debra Bromson

Assistant General Counsel
AAA Club Alliance Inc.
DBromson@aaamidatlantic.com

K Royal

Associate General Counsel
TrustArc Inc
Serious Privacy podcast
kroyal@trustarc.com

Maggie Gloeckle

Associate General Counsel, Head of Global Privacy
A + E Networks
margaret.gloeckle@aenetworks.com

Wayne Unger

Founding Attorney, The Unger Firm LLC
Visiting Assistant Professor of Law, Gonzaga University School of Law*
wayne@ungerfirm.com

*Starting Fall 2021