Building an effective feedback loop for your privacy program through Privacy Incident Response

PEPR ‘20 October 2020

Sri Maddipati
Privacy Engineer
1.0

Introduction
Building a privacy program

1. Privacy policies
2. Risk Assessment and Compliance
3. Privacy by design
4. Incident Response
2.0

Privacy IR
Why is it challenging regardless of organization scale?

- Limited channels for incident detection
- Notification obligations
- Managing long term remediation and prevention
- Privacy budget/resources
The Feedback loop

- Identify the threats, vulnerabilities and risks
- Metrics, Trend analysis - Incident remediation and prevention
- Detect and respond to incidents
- PIAs, audits, and vendor assessments
- Privacy focussed SDLC

Detect and respond to incidents
3.0 Privacy Metrics
Why metrics matter?

1. See the big picture
2. Identify scope for improvement
3. Justify the need for resources
4. Highlight effectiveness of IR
5. Incidents prevention
Things to consider

1. Data Quality
2. Consistency in tracking metrics across the organization
3. Measuring privacy health using metrics - What are the blind spots?
4. Choosing the right audience to share metrics.

"Errors using inadequate data are much less than those using no data at all."

– Charles Babbage
What metrics matter?

- Volume/Spike in incidents
- Incident source - external vs internal
- Trends - by service/product, type of privacy issue, incident severity, root cause
- Third Party/Vendor related
- Incident Impact - # of affected users
- # of Incidents vs Events
- # of incidents with notification obligations
Thank you!