The Privacy Rosetta Stone: How to Make Yourself Understood by the CISO and CIO

Recorded on: 4 October, 2019
Welcome & Introductions

Host:

Dave Cohen
CIPP/US, CIPP/E
Knowledge Manager
IAPP

Speakers:

Sophie Chase-Borthwick
Director of Data Ethics and Privacy
Calligo

Adam Ryan
Chief Operations Officer
Calligo

Dana Simberkoff
CIPP/US
Chief Risk, Privacy and
Information Security Officer
AvePoint Inc.
The Problem
The Problem

What it is

• The common inability for privacy professionals to communicate and collaborate effectively with their CIOs and CISOs.

How it has come about

• Most privacy pros come from either a legal or compliance background. Not technical.
• Literally speak a different language to CIOs and CISOs – same words, different meanings.
• Because of their typical backgrounds, privacy pros often focus too much on the legal nuances, not the practical implementation.
• Meanwhile, privacy laws are driving an increasingly technical agenda, with concepts such as privacy by design.
• Crucial mismatch.

Why it is dangerous

• Privacy laws were updated because technology was outrunning privacy protections.
• Whole concept of privacy is based on data – inherently technical.
• For privacy pros not to be able to discuss technical practicalities with their CIO / CISO misses the entire point of data protection.
How to Spot When You Have this Problem
Symptoms of a Bad Relationship

- Compliance and legal teams have little day-to-day interaction with CIO and CISO
- Privacy is considered a “blocker to business”
- Execution of Data Subject Rights ends up being manual and onerous
- Personal data is practically impossible to delete or anonymise due to infrastructure
- Privacy notices bear no resemblance to what is actually done
- Breaches are difficult to evaluate & understand
Symptoms of a Good Relationship

- Common aims and regular working relationship between privacy and CISO / CIO (even if translation is still often required)
- Privacy genuinely built into business practices meaning it is less likely to hinder business practices and more likely to be effective
- Data Subject Rights are easier to address / action / administer
- Breach assessments are quick as combined team understands the nature of the security incident, its ramifications & the risk to data subjects
- More innovative as focus is on the goal of the project, not on team dynamics
How the Language Barrier Has Foiled Our Clients, and What They Do Now
Client Example 1

Client situation:

- IoT database
- Also used for sales analytics and as a marketing database
- Emails as primary key

Problem 1: Privacy requires right to erasure. Because it was a combined database, and email was the primary key, then removal of any subject’s entry meant it was lost for analytics too. Blocker to business.

Problem 2: No separation of marketing preferences from other data sets – consent was impossible to implement.

Resolution: Separate tables within data warehouse for different use, plus random generated primary key.

Result 1: Data subject rights now easy to enforce, and erasure is simple and protects wider use.

Result 2: Marketing preferences easier to record / adjust with new programs.
Client Example 2

**Client situation:**
- Company security measures and performance monitoring involved monitoring of employees’ activity (BYOD, service desk stats, internet monitoring etc.) via a 3rd party SaaS.

**Problem 1:** Were gathering vast amounts of data without knowing what they were going to use it for, or explaining to employees what was being done.

**Problem 2:** Personal data of employees is not considered as a part of a 3rd party contract.

**Problem 3:** Statistics were available to a wide array of internal teams.

**Resolution:** Employee contracts urgently renegotiated.

**Result 1:** Usage defined and project tailored to only collect the personal data genuinely required for the purpose.

**Result 2:** Reduced audience, but more suitable protection.
Client Example 3

Client situation:

- Misunderstandings over meaning of “security incident” and “potential personal data breach”.
- In IT & Security (also ITIL) an “incident” does not necessarily mean a “breach”, at least not as a Privacy pro would understand it.
- Also means a “Potential” breach e.g. an unexploited vulnerability.

Problem 1: Security articulated an “incident”. However, Legal and Compliance automatically mentally went to “breach” and reacted accordingly. Took multiple hours for them to understand nothing had yet happened, & then evaluate risk appropriately.

Resolution: Literal translation between the two sides, as though speaking foreign languages.

Result: Ongoing education to allow actual departmental nuances to be considered in future.
Top Tips
What not to do

- See the other departments as “the other side”
- Assume your language is the correct one
- Assume someone else will understand what you are saying

What to do

- Talk to your teams, build relationships and find out:
  - What they do
  - What their aims are
  - What they fear
  - How they communicate amongst themselves
  - Share “Your job for dummies”
- For all projects, talk up front during design phase and be united and comfortable in the joint approach
- Establish regular catch ups between the disciplines for current & upcoming activities
- Agree to a common vocabulary within your organization (“Ensure”, “Incident”, “Erasure”, etc)
Want to talk further?

Contact Sophie:

sophie.chase-borthwick@calligo.cloud

Check out our website:

https://calligo.cloud/services/data-privacy-services/
Panel Discussion

Host:

Dave Cohen
CIPP/US, CIPP/E
Knowledge Manager
IAPP
dave@iapp.org

Speakers:

Sophie Chase-Borthwick
Director of Data Ethics and Privacy
Calligo
Sophie.Chase-Borthwick@calligo.cloud

Adam Ryan
Chief Operations Officer
Calligo
adam.ryan@calligo.cloud

Dana Simberkoff
CIPP/US
Chief Risk, Privacy and
Information Security Officer
AvePoint Inc.
Dana.Simberkoff@avepoint.com
THANK YOU!

To our speakers, our sponsor, and to all of you in the virtual audience.

Marketing Preferences

This web conference is being provided to you free of charge thanks to the generous support of our sponsor. In exchange for this support, we provide the sponsor with registrant contact information under strict guidelines. If you would like to opt-out of being contacted by our sponsor, you may express your preferences here: privacy@calligo.cloud.
Web Conference
Participant Feedback Survey

Please take this quick (2 minute) survey to let us know how satisfied you were with this program and to provide us with suggestions for future improvement.

Click here:

https://www.questionpro.com/t/AOhP6ZeYUf

Thank you in advance!
For more information: www.iapp.org
Attention IAPP Certified Privacy Professionals:
This IAPP web conference may be applied toward the continuing privacy education (CPE) requirements of your CIPP/US, CIPP/E, CIPP/G, CIPP/C, CIPT or CIPM credential worth 1.0 credit hours. IAPP-certified professionals who are the named participant of the registration will automatically receive credit. If another certified professional has participated in the program but is not the named participant then the individual may submit for credit by submitting the continuing education application form here: CPE credit application.

Continuing Legal Education Credits:
The IAPP provides certificates of attendance to web conference attendees. Certificates must be self-submitted to the appropriate jurisdiction for continuing education credits. Please consult your specific governing body’s rules and regulations to confirm if a web conference is an eligible format for attaining credits. Each IAPP web conference offers either 60 or 90 minutes of programming.
For questions on this or other IAPP Web Conferences or recordings or to obtain a copy of the slide presentation please contact:

Dave Cohen, CIPP/E, CIPP/US
Knowledge Manager
International Association of Privacy Professionals (IAPP)
dave@iapp.org
603.427.9221