RSAC 2025 Conference

Many Voices.
One Community.

SESSION ID: PDP-W08

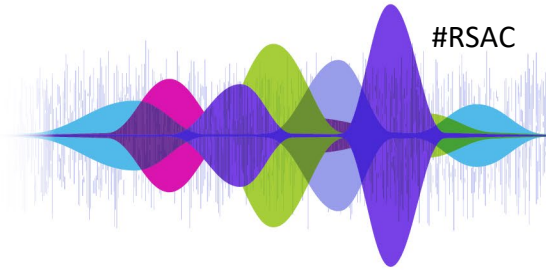
Amplifying Success: How Security and Privacy Teams Break Barriers Together

Edy Glozman

Vice President of Legal
Axonius
linkedin.com/in/edy-glozman

Lenny Zeltser

Chief Information Security Officer
Axonius
linkedin.com/in/lennyzeltser



Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

I Want YOU… as the DPO

Data privacy professionals safeguard people's personal data.

- Data Subject's choice and control
- PII and other personal data classification
- Privacy laws and regulations
- Key Principles
  - Lawfulness, fairness, transparency, purpose limitation
  - Data minimization, integrity, confidentiality

Cybersecurity safeguard the company's systems and data.

- Confidentiality, integrity, availability
- Threats and vulnerabilities
- Secure software development practices
- Monitoring, response and investigations

Different focus areas and expertise, but lots of room for alignment and collaboration.

Example #1: Security Monitoring

Misalignment of Interests

Security Wants

- Full visibility into “everything”
- Data kept “forever” for investigations

Privacy Wants

- No visibility into PII
- No PII data retention

“You have no expectation of privacy.”

- A common phrase in Acceptable Use Policies in US companies
- Unacceptable to people in other countries, including the EU
- How to address the requirements in a global company?
- Privacy laws are dynamic: Schrems I & II

Resolution

- Documented specific monitoring scenarios and their benefits.
- Ensured that violations are prohibited via the Acceptable Use Policy.
- Investigated legal privacy exposure for each scenario to make an informed risk decision.
- Set up checks and balances, so the legal team has visibility into the security settings and activities to deter abuse.
- When interests are misaligned:
  - Understand the underlying needs/priorities of the other party.
  - Work collaboratively on a compromise.

Example #2: Data Collection and Retention

Alignment of Interests

Security Wants

- Less data about data subjects
- The less data we have, the smaller our security exposure

Privacy Wants

- Less data about data subjects
- The less data we have, the smaller our privacy exposure

Alignment of Interests

Business Wants

- Retain past employees' files, emails, and other data for a long time
- Ensure smooth transitions when people leave the organization

Security and Privacy Want

- Minimize or eliminate retention of data that might include PII
- Meet privacy requirements
- Decrease the attack surface

Legal and Privacy: Internal Conflict

- "Legal" and "Privacy" needs might be at odds.
  - "Legal hold": Legal requirements for litigation require keeping data for a long time.
  - Sarbanes-Oxley Act (SOX) requires companies to preserve certain financial data for a long time.
- This could conflict with privacy requirements for data retention.
- The legal professional acting as General Counsel and DPO must understand which need governs, or, if the weight is "equal," find the right balance.

Resolution

- Tiered system for employee data retention; business justification for keeping “VIP” employees’ data longer.
- Automated processes for enforcing data retention decisions
- When interests are aligned, strengthen the relationship:
  - Work together to understand data collection, flows, and storage.
  - Use alignment of interests to strengthen the relationship; collaboration that helps resolve future “conflicts.”
  - “United front” approach vis-a-vis business requests that are overly risky.

Example #3: Data Breach and Incident Response

Distinct Responsibilities

Security Handles

- Investigating security events
- Responding to security incidents
- Determining the affected resources
- Performing technical analysis

Legal and Privacy Handle

- Understanding legal and contractual repercussions
- Determining notification and related obligations
- Outcome is not always binary, there is room for interpretation

The Need to Collaborate and Negotiate

Security Wants

- Early and frequent updates
- Transparency to retain trust

Legal and Privacy Wants

- Minimize the released details
- Safeguard from future litigation

Resolution

- Documented responsibilities in the incident response policy.
- Built a collaborative relationship through aligned interests.
- Practiced decision-making during low-severity incidents and tabletop exercises.
- Captured the need to decide whether to notify the affected parties even if there is no legal requirement to do so.

Example #4: Procurement of Software With AI Capabilities

Overlapping Perspectives

Security Asks

- Might our confidential data leak to unauthorized parties?
- What safeguards exist for data protection?

Privacy Asks

- Might our PII leak to unauthorized parties?
- What safeguards exist for privacy protection?

AI Governance

- Privacy professional often have AI governance responsibilities.
- Catalog the way in which AI is used internally to address customers' questions.
- Understand on what data the AI model was trained and the risk of IP infringement.
- Ensure employees understand their responsibilities for using AI.

Resolution

- Included AI review in the procurement process, posing questions to the buyer and the vendor.
- Published an internal guidelines document that explains AI usage expectations to employees.
- Catalogued the use of AI within the company.

Stronger Together

Categorizing Privacy and Security Interactions

Distinct Questions	Same Questions	
	Interests Aligned	Interests Not Aligned
Ex #3: Data breach (Cybersecurity Q: *What happened?* | Privacy Q: *What are the legal obligations?*) Ex #4: AI Tooling (Privacy Q: *How do we govern AI?* | Cybersecurity Q: *How do we avoid leakage of data?*)	Ex #2: PII collection (Same Q: *What is the appropriate time for data retention?*)	Ex #1: Security monitoring (Same Q: *Can we monitor employee data?*)

Apply This: Framework for Collaboration

Step 1: Identify whether the questions each practitioner needs to tackle are similar or distinct:

- If distinct, each practitioner should take the lead/ownership of the answer to their respective question.
- If similar, move to Step 2.

Step 2: Consider whether the interests are aligned:

- If aligned, drive together to a resolution
- If not aligned, negotiate a solution generally satisfactory to both parties, noting that “a solution” is better than “no solution.”

Situational Awareness

Do

- Recognize the specific dynamics of each scenario.
- Stay curious and expand your expertise in multiple domains.
- Build trust when the interests are aligned for future situations.
- Be a collaborative negotiator when interests are not aligned

Don’t

- Focus solely on your own job and perspective.
- Discount the expertise and responsibilities of your colleague.

RSAC™ 2025 Conference

Many Voices.
One Community.

Thank you!