ObservePoint EDGE

MUNAWAR
VALIJI

CYBER SECURITY EXPERT

JELLYCAT® LONDON

About Me: Mun Valiji

- 25 years Practitioner Security, IT Risk and Privacy
- Last 12 years advising FTSE 250 Boards
- Leading front line cyber battle
- Senior Advisory Council Info Sec Europe
- NCSC & NCA Community Lead
- Cyber Startup Advisor
- Dad of two (princesses)

Lisbon - City of Spies

- During World War II, spying flourished in Lisbon, the main point of entry into and exit from Europe.
- One **fascinating fact about Lisbon** is that the city is connected with the spying history of the time.
- A British writer, Ian Flemming, who **created James Bond**, was a spy stationed in Lisbon working for the British Secret Service.
- The Estoril Casino on the Portuguese Riviera inspired him to write his first book, Casino Royale.
- **Tenuous** link to Privacy and Compliance

Customer is King => Build Trust

Transparency is essential for building and maintaining user trust.

When companies are open about their data collection and usage practices, security measures, and policies, users are more likely to trust the platform and feel comfortable using it.

In the new and changing world of data privacy regulations, it's clear that data protection is a major public concern.

We are continuously challenged to **proactively secure** data collection on websites and protect customers and their data.

(Cookie) Governance: Importance

The primary objective of cookie governance: **‘minimize the data collected and ensure that cookies are used only for their intended purpose.’**

Rise of data breaches and privacy concerns, it has become increasingly important to manage cookies responsibly.

The use of cookies can raise legal and ethical issues. To ensure compliance with **General Data Protection Regulation** (GDPR) and the **California Consumer Privacy Act** (CCPA), websites must implement effective cookie governance strategies.

For most FTSE 250 Boards Data Privacy remains a top 3 risk

Dedicated Privacy specialists are aligned to engineering and product teams

(Cookie) Governance: Must Do

Use a **dedicated** cookie management solution. Platforms **automate** consent records collection, storage and management so you can consistently apply user preferences across your organisation.

Design user **friendly** forms. Users should easily **understand** and engage.

Regularly **review** consent practices. Periodically **audit** your practices to ensure **alignment** with standards.

Training and awareness: **Educate** your staff through regular training and awareness programs

GDPR Compliance: Landscape Outlook

GDPR regulators have been busy. They issued hundreds of fines to companies, including Google and Facebook, more than **€114 million** in the first 20 months of GDPR.

Developments, like Brexit, other countries introducing their **own data protection laws**, and rulings from the Court of Justice of the European Union.

For the largest tech companies to truly take data protection seriously, experts think that the fines will need to be **much higher**.

Margarethe Vestager, head of the European Commission, has called for **stronger enforcement of the GDPR** and policies that promote competition in the tech industry.

Website Privacy & Trust Validation: Good Practice

Good Consent Management Platforms should scan your website cookies for **functionality** and **privacy** risks. Some key considerations:

- Perform pre-scheduled website scans to discover and categorize cookies.
- Collect and store consent based on categories (e.g., strictly necessary, analytics, targeting, etc.)
- Maintain **audit** logs to record and track cookie banner settings and preferences modifications.
- Display data with an accessible, **easy-to-navigate** user interface.
- Build **dashboards** for your executive team to monitor and track consent status.

Frequency? Monthly / Quarterly? Depends on number of **changes** and **resources** + organisational maturity.

Focus on **reporting**, **analysis** and **automation**.

Continuous Security & Trust Validation

Take a **proactive** approach involving consistent assessment and validation of security controls and functionality for **prioritized** remediation actions.

Identify any **gaps** and **defects**, thereby enabling **mitigation** of identified gaps and validate the effectiveness of security and privacy measures.

Taking a **proactive** approach helps you stay **ahead** of changes and defects which may adversely affect your business.

Help to identify **policy** mismatches in controls by **simulating** and determining where controls maybe lacking and misconfigured.

In Conclusion

Customers demand trust and privacy

Compliance landscape will become more **complex**

Adopt a lean tool-based approach to reporting and managing compliance

Take a collaborative, **risk-based** approach to consent

Thank you.