

Your data is out there  
somewhere...

Probably having a better time than  
you



With you today

**Kameliya Stoeva**  
Manager Cybersecurity

🎾 Tennis enthusiast

“

90% of organizations store sensitive data in the cloud — yet only 12% encrypt it end-to-end. Now add AI access on top of that.

→ **54% of data in the cloud is sensitive (was 47% in 2024)**

- Data Security, AI governance, and Identity & Access Management **should be** more connected than ever



One GenAI query can unlock years of sensitive company data — in seconds



IAM is your passport control = shrink what any identity can see, ask, or share



Data's trip: Private systems → Vendor cloud → External AI Tool

Private Systems

- Owner-held keys
- Least privilege
- Audited access



Trust boundary  
(what you fully control)

Third Party Cloud



vendor's cloud breached



Vendor/AI boundary  
(shared control)

External AI Tool



AI Model

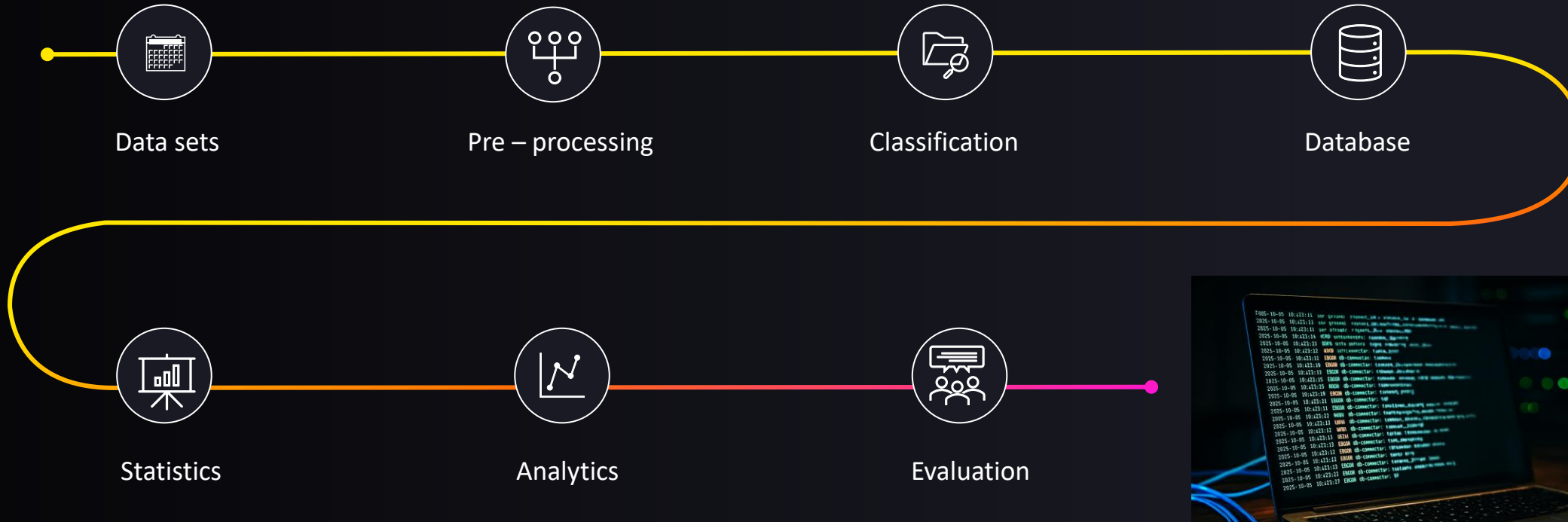


**Shared-responsibility risks:** vendor retention/training on your data, log copies of your data  
**Cross-tenant risks:** prompt/data leakage, tenant misconfiguration

**Exposure Surface**  
(outside our control)

If your internal data-mining tool can see authorizations, Segregation of Duties (SoD), and privileged access—so can whoever compromises it.

## Internal data-mining pipeline



### Exposure Surface (outside our control)

- Data is share outside of the system
- Logs capture sensitive data
- Data copied to backups is hard to fully remove

# Key takeaways

## Move fast on AI—privacy by design

- Tag sensitive data
- Set limits on data exports
- Keep records of inputs and outputs of data

## Tighten IAM

- Define default to least privilege access
- Scope what identities can ask and see
- Review high-risk roles monthly

## Protect data in motion

- Use data labels and data loss prevention (DLP) tools.
- Store data only briefly — don't keep it longer than necessary
- Regularly check and sanitize data files for sensitive information

**Thank you!**