SafeLiShare Dynamic
Data Security Lifecycle

Cybersecuity and Privacy Risk Relationship

Cyber Security Risks
Associated with cybersecurity incidents arising from loss of confidentiality, integrity, or availability

Cyber Security-related privacy events

Privacy Risks
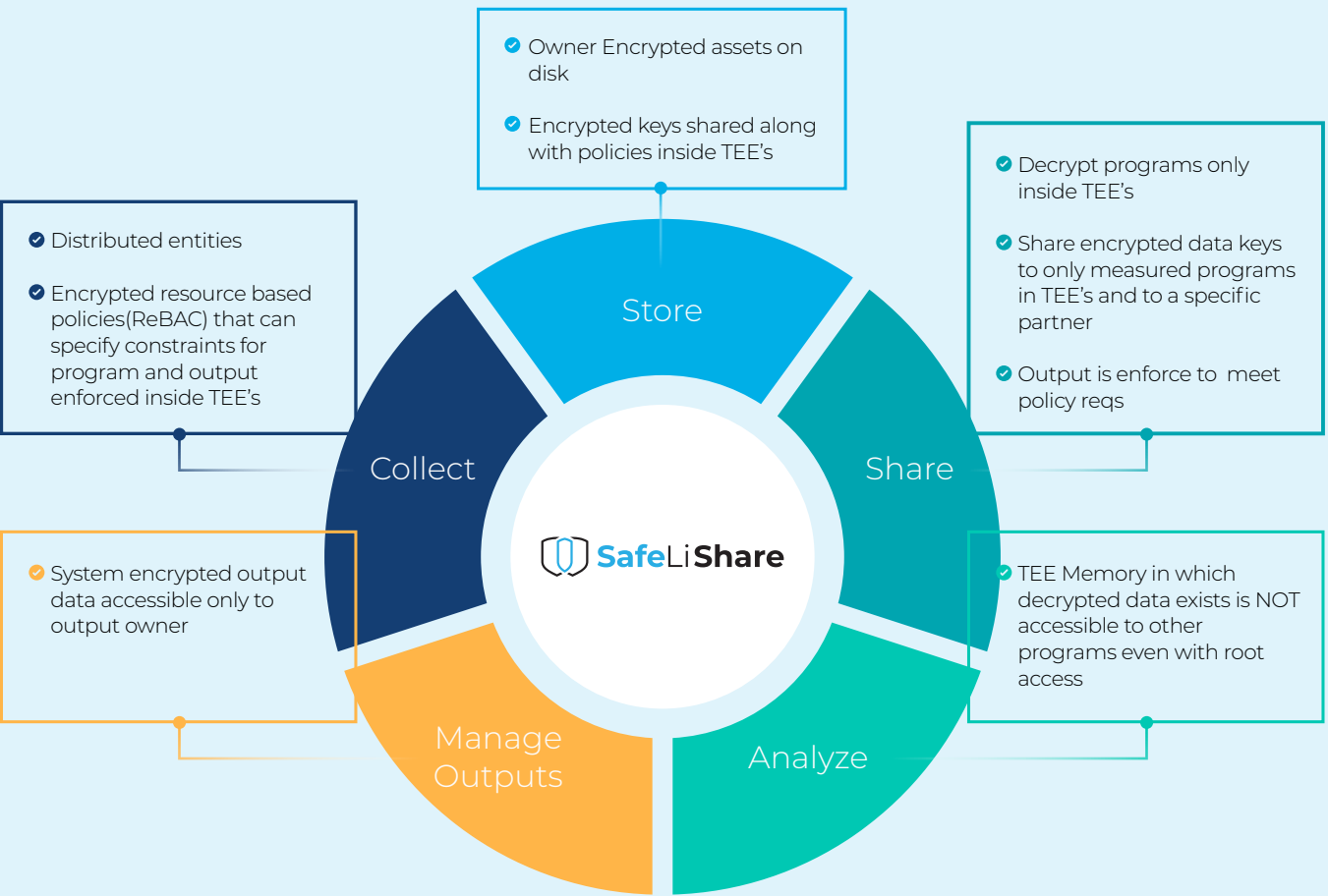Associated with privacy events arising from data processing
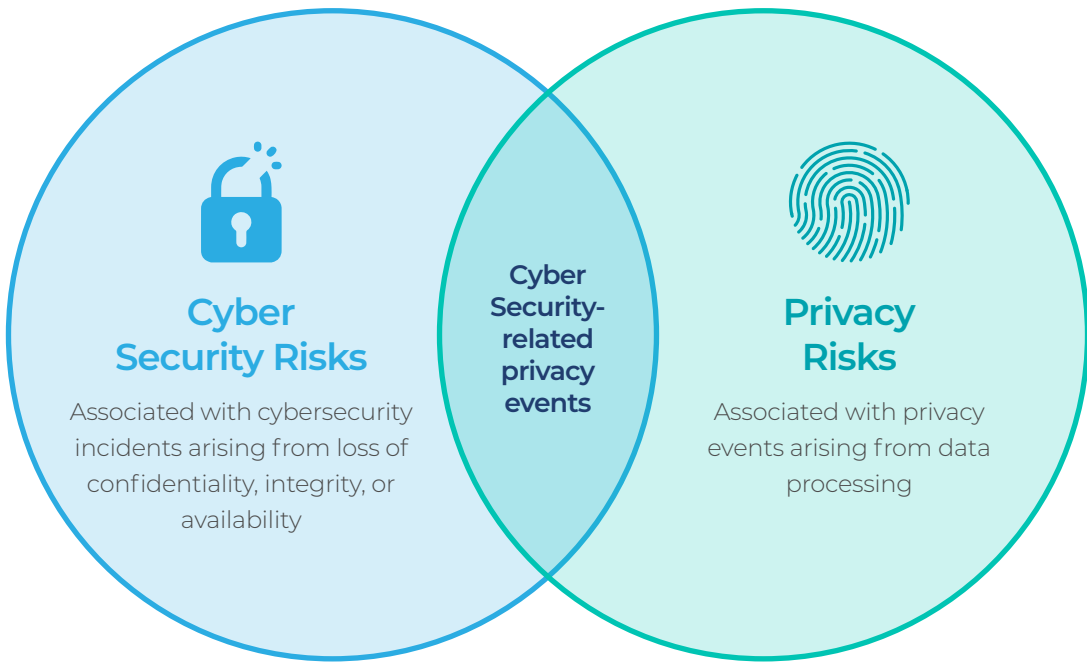
A data life cycle operation with data processing, including the following data actions, but not limited to:

- ✓ Collection
- ✓ Logging
- ✓ Transformation
- ✓ Disclosure
- ✓ Transmission
- ✓ Retention
- ✓ Generation
- ✓ Use
- ✓ Sharing
- ✓ Disposal
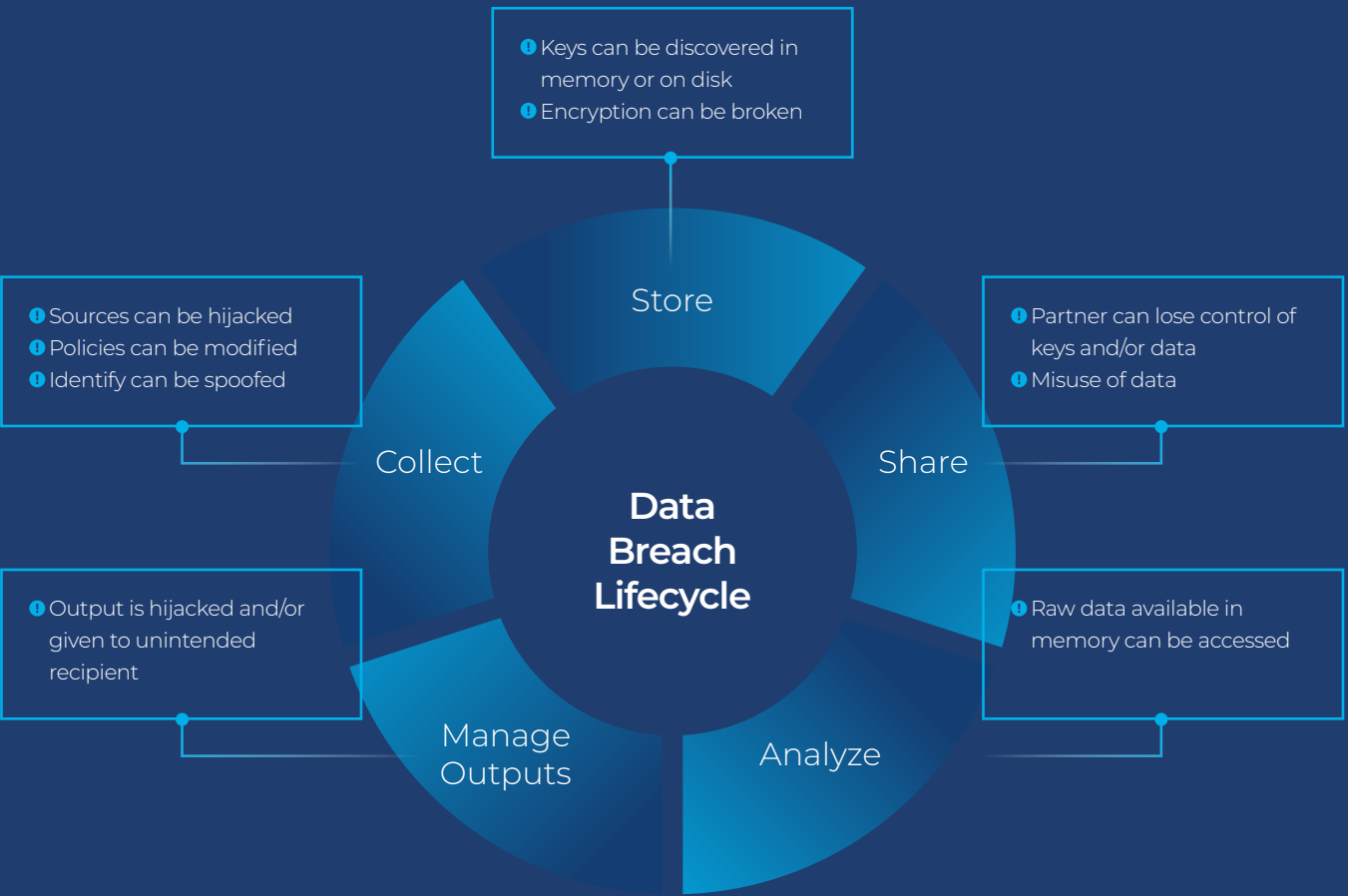
Data Breach Lifecycle

Store
- ❶ Keys can be discovered in memory or on disk
- ❶ Encryption can be broken

Collect
- ❶ Sources can be hijacked
- ❶ Policies can be modified
- ❶ Identify can be spoofed

Share
- ❶ Partner can lose control of keys and/or data
- ❶ Misuse of data

Manage Outputs
- ❶ Output is hijacked and/or given to unintended recipient

Analyze
- ❶ Raw data available in memory can be accessed

1 Collect	2 Store	3 Share	4 Analyze	5 Manage Outputs
· Verify Data Sources · Identify Protected Data · Create metadata · Assign ownership and policies	· Save data · Provide access to only approved actors	· Provide data to partners and Programs	· Run compute on data and produce output	· Provide access to outputs

SafeLiShare Application Data Lifecycle

Store
- ✓ Owner Encrypted assets on disk
- ✓ Encrypted keys shared along with policies inside TEE's

Collect
- ✓ Distributed entities
- ✓ Encrypted resource based policies(ReBAC) that can specify constraints for program and output enforced inside TEE's

Share
- ✓ Decrypt programs only inside TEE's
- ✓ Share encrypted data keys to only measured programs in TEE's and to a specific partner
- ✓ Output is enforce to meet policy reqs

Manage Outputs
- ✓ System encrypted output data accessible only to output owner

Analyze
- ✓ TEE Memory in which decrypted data exists is NOT accessible to other programs even with root access

1 Collect	2 Store	3 Share	4 Analyze	5 Manage Outputs
· Verify Data Sources · Identify Protected Data · Create metadata · Assign ownership and policies	· Save data · Provide access to only approved actors	· Provide data to partners and Programs	· Run compute on data and produce output	· Provide access to outputs