(d) 3. Privacy Policy Development Approach and Workplan

Smart Cities and Service Improvements Committee
September 5, 2019

Dolan Beckel, Director, Office of Civic Innovation
J. Guevara, Broadband Manager, Office of Civic Innovation
Sarah Zárate, Assistant to the City Manager

Why have a Privacy Policy?

A Citywide Privacy Policy is crucial **to safeguard and protect the public's trust** as the City increasingly **adopts new technologies** to better serve our residents.

Our Purpose for Privacy Policy

To **develop an overarching Citywide Privacy Policy** that operationalizes the City's Privacy Principles, and to **establish a sustainable privacy governance model**.

From Privacy Principles to Privacy Policy

A Look Back…

- Privacy Principles Accepted on June 6, 2019
  - Referred to City Council
- Harvard Recommendations
  - Start with Privacy Principles
  - Ground in Community Engagement
- City Approach
  - Robust Community Engagement
    - ✓ Internal Working Group, Advisory Task Force, Community Meetings
  - Developed Privacy Principles
    - ✓ Principles approved by Committee in June, headed to Council September 17th

From Privacy Principles to Privacy Policy

Developing a Work Plan for FY 2019-2020

- Scan of City Landscapes
  - Identification of leading cities
    - ✓ New York City, City of Chicago, City of Seattle

City	Privacy Policy	Privacy Principles	Other
Austin, Texas	No	No	Playbook Model – focus on design
Boston, MA	No	No	IoT projects have specific policies
Chicago, IL	No	No, but "principled approach: transparency and public engagement	-Voluntary efforts -Privacy-by-design
NYC	Yes, baseline	Yes	-IoT guidelines -Interest in Seattle Program
Oakland, CA	No, but have use policies	Yes	-Equity Principle
Seattle, WA	Yes	Yes	-Full program -Equity statement

From Privacy Principles to Privacy Policy

Developing a Work Plan for FY 2019-2020

- **City of Seattle**
  - Considered the leader in privacy
  - Began working on privacy in 2015
  - Have a full Privacy Program, 3 FTE, $800,000/year
  - Grounded in city's equity work

From Privacy Principles to Privacy Policy

Developing a Work Plan for FY 2019-2020

- **National Institute of Standards and Technology (NIST)**
  - Privacy Framework Standards
  - Based upon Cybersecurity Framework
  - Risk-based and flexible across any organization
  - Version 1.0 due by end of 2019

From Privacy Principles to Privacy Policy

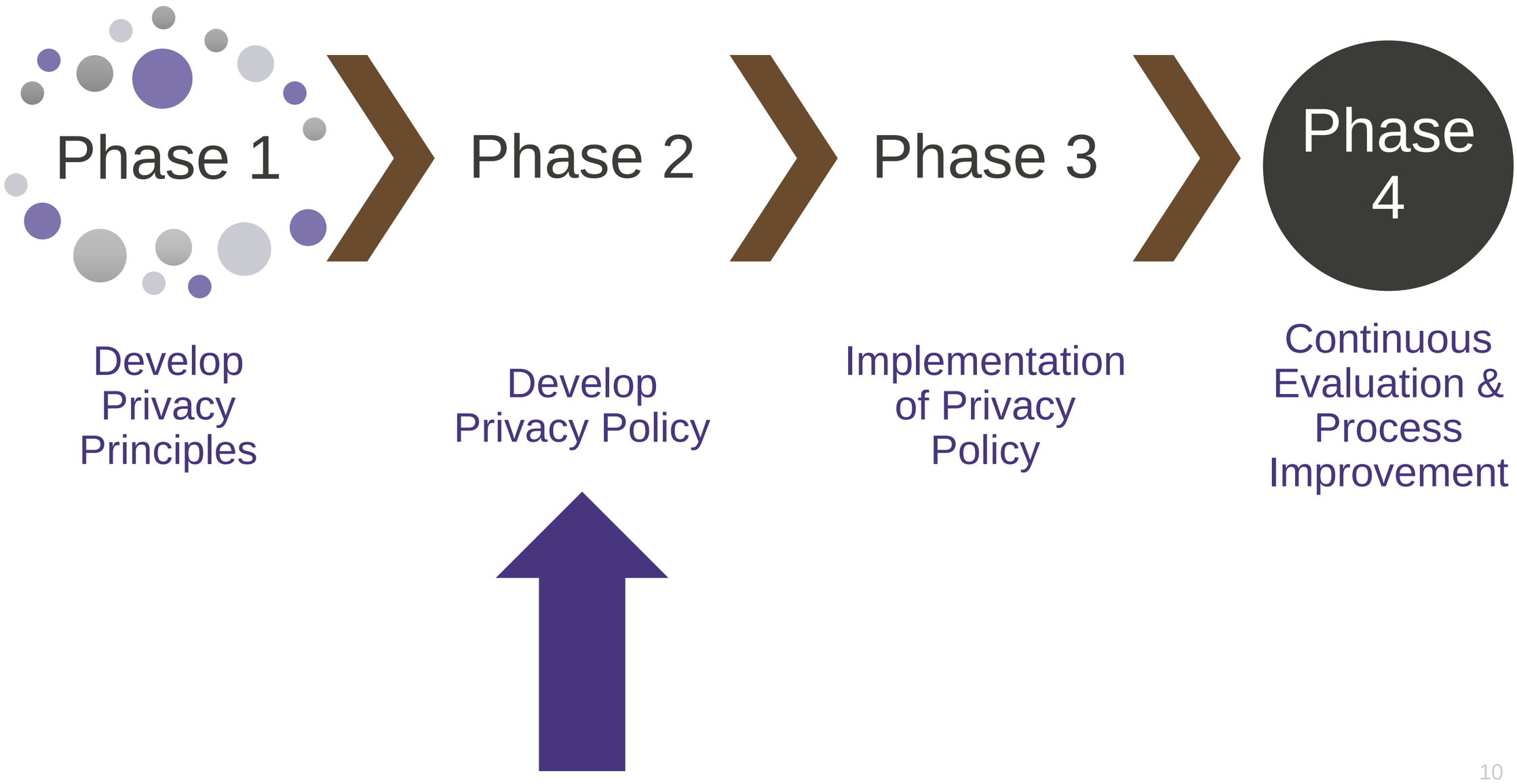
Developing a Work Plan for FY 2019-2020

- General Data Privacy Regulations (GDPR)
  - Leading legislative framework
  - Applies to public and private entities
  - Exceeds the California Consumer Privacy Act (AB 375)
  - Partnership with the City of Dublin, Ireland

Moving Forward…

We want to **leverage other cities' experiences** and lessons learned, but **create a product** that is **unique to San José's needs.**

From Privacy Principles to Privacy Policy



Our Approach

The City plays an important role in ensuring the protection of the populations its serves, and especially in ensuring it neither creates nor perpetuates structural inequities.

Grounded in this value, the **policy development process will ensure the inclusion of community voices** to help guide how (and what) data is collected and used.

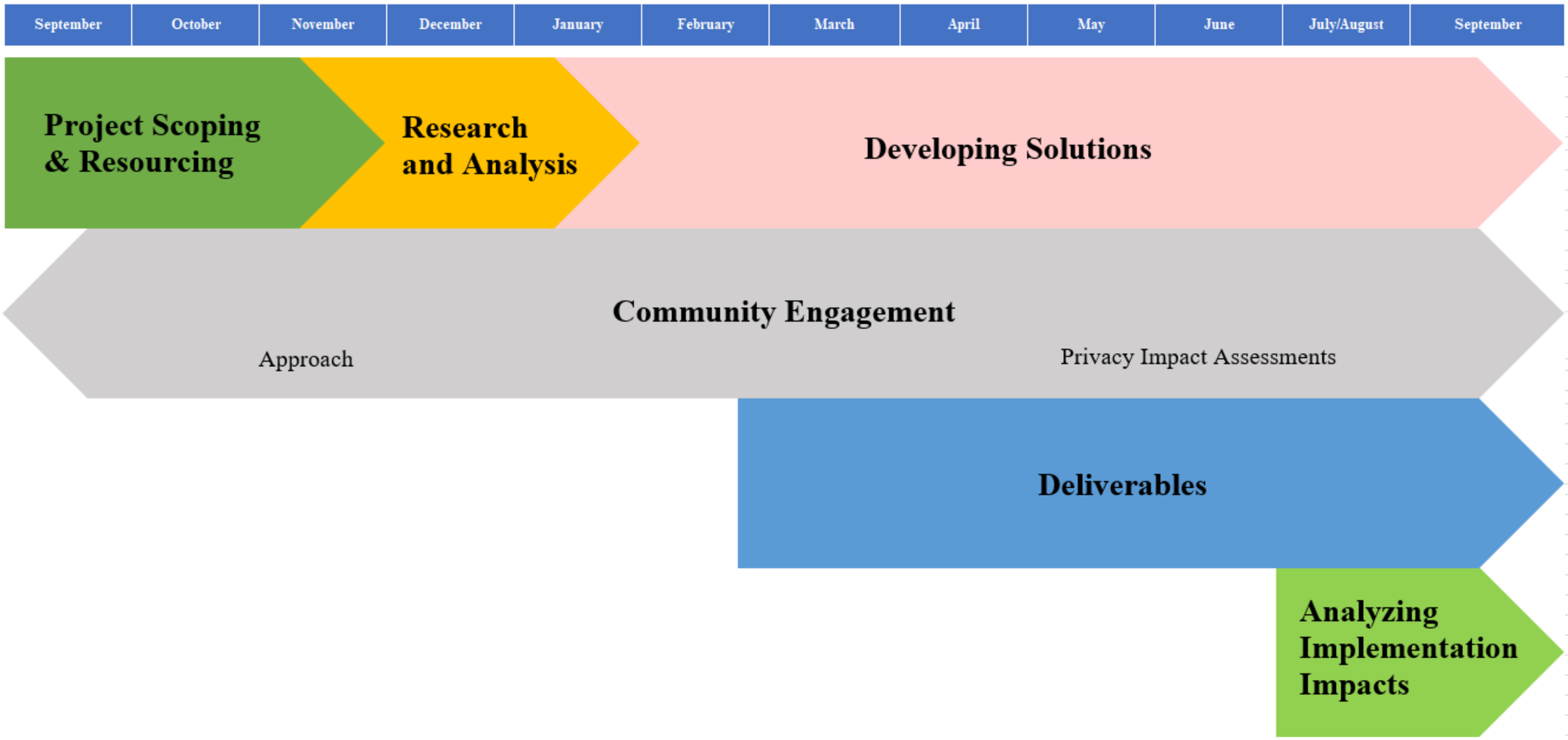
From Privacy Principles to Privacy Policy

Phase 2 Deliverables*

- *Citywide Privacy Policy*
- *Citywide Data Retention Schedule*
- *Privacy Impact Assessment Toolkit*
- *Training Framework for City Departments*
- *Master List of Sensing Technologies*
- *Sustainable Privacy Governance Model*
- *Stakeholder Engagement for Guidance and Feedback*

**Deliverables are based on research through August 2019*

From Privacy Principles to Privacy Policy



(d) 3. Privacy Policy Development Approach and Workplan

Feedback and questions

Leveraging GDPR and CCPA

General Data Protections Regulations (GDPR)

- Mandatory breach notification (Covered under other California laws)
- Data Protection Impact Assessment (DPIA)
- Governance specific requirements
- Privacy by Design (PbD)
- Supervisory/regulatory authority authorization for certain types of processing
- Mandatory Data Protection Officer (DPO)
- Requirements specific to data processors
- Cross-border transfer requirements
- Processing bans
- Supervisory authority right to audit
- Restrictions specific to automated decision making

California Consumer Privacy Act (CCPA)

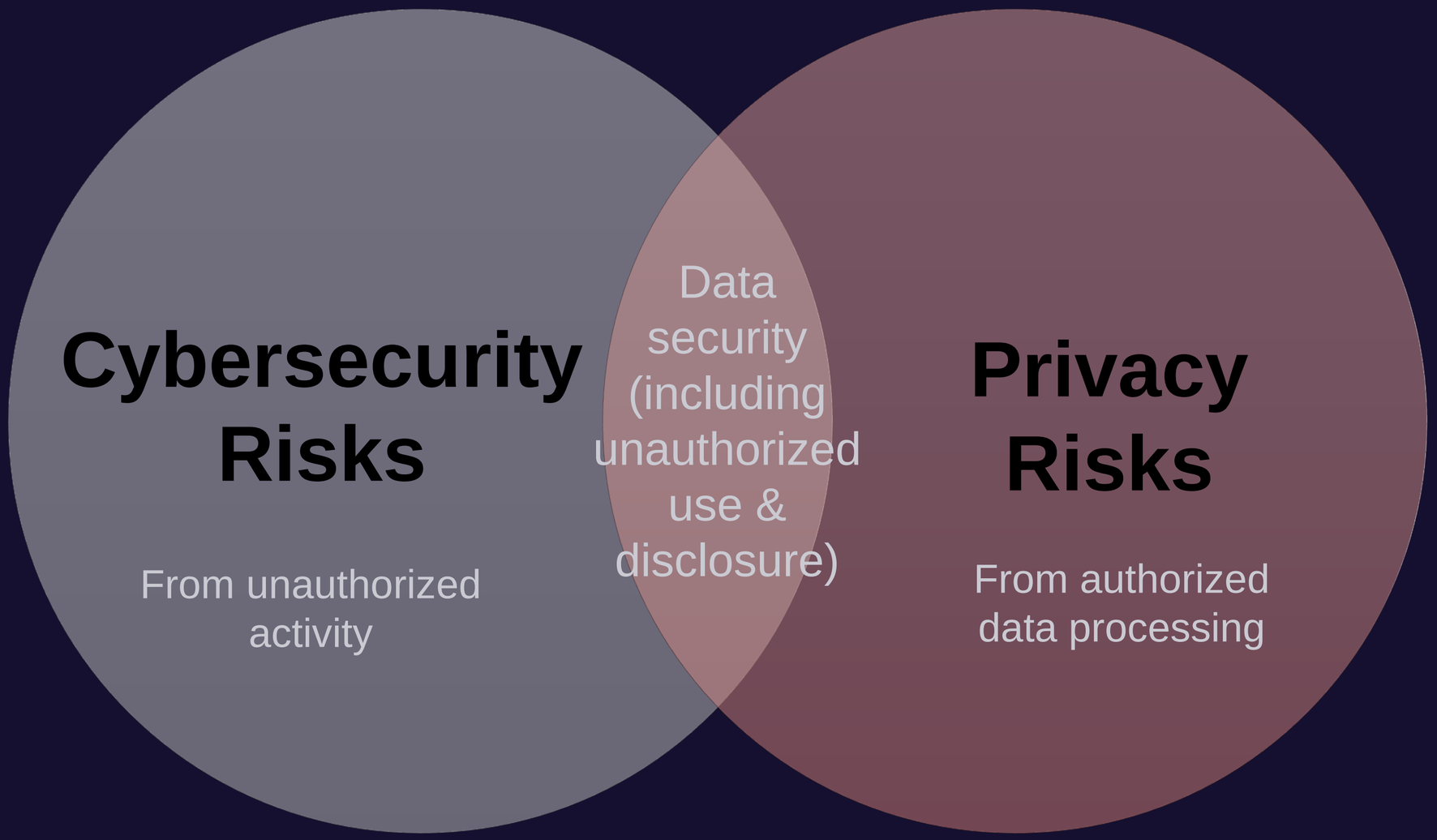
- Right to limit the sale of Personal Information (PI)
- Unable to discriminate the services or products provided based on option out on the sale of Personal Information (PI)

- Training
- Notice*
- Consent*
- Access and portability
- Erasure
- Right to object
- Right to rectification
- Aspirational requirements related to security
- Encryption or redaction of Personal Information (PI)

* Although required by both the CCPA and GDPR, there are specific requirements to demonstrate compliance with the CCPA

Based on 2018 Deloitte slide presentation

Cybersecurity and Privacy Risk Relationship



Based on “Getting to V1.0 of the NIST Privacy Framework: Workshop #3 July 8, 2019