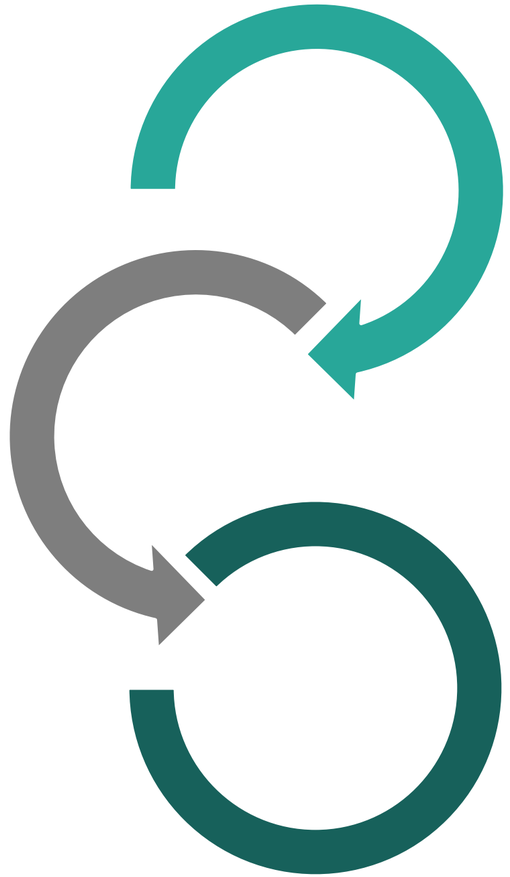
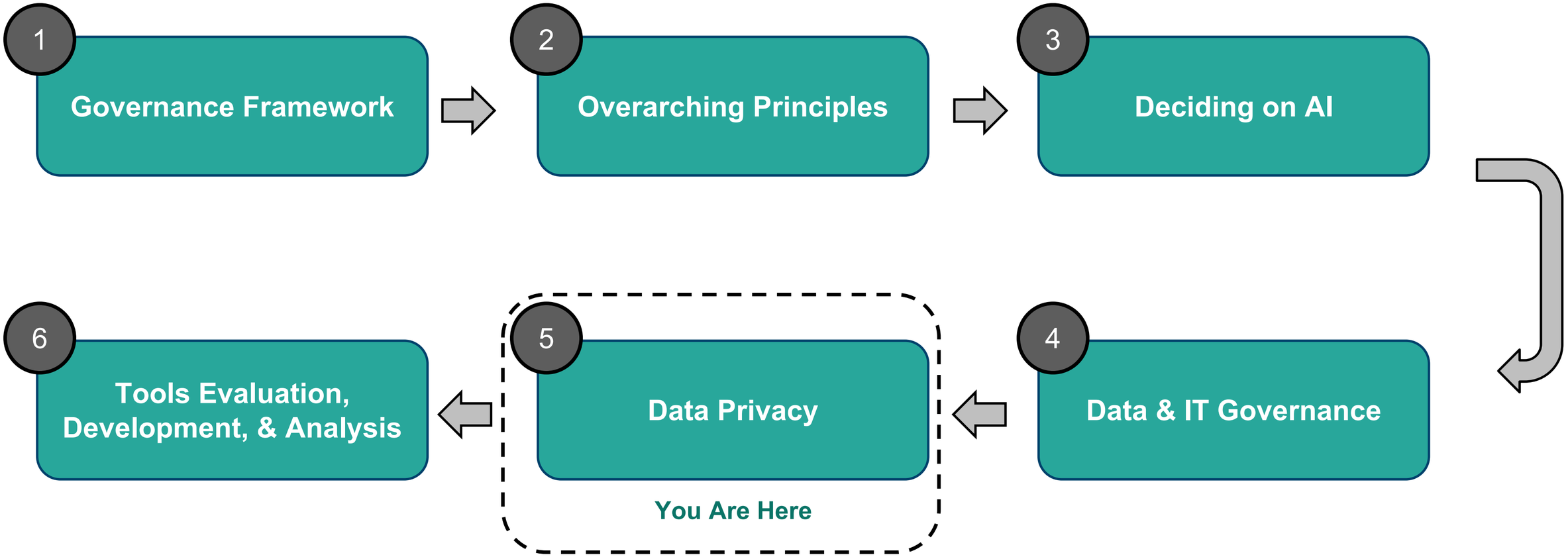
Data Privacy



Presented by ANB Advisory Group
Afua Bruce and Rose Afriyie

Six modules will guide you through important considerations for nonprofits when implementing AI



At the end of this module, you will…

- Understand how privacy principles extend to AI
- Receive recommendations on data access and permissions
- Learn best practices on AI and privacy

Data privacy refers to the norms & practices that help to safeguard human autonomy, identity, and dignity *

These norms and practices typically address:

- Freedom from intrusion
- Limiting observation
- Individuals' agency to consent to disclosure or control of facets of their identities (e.g., body, data, reputation)

NIST has long been a leader in the privacy domain. Their definition of privacy and norms is excerpted from pg. 17 of their Artificial Intelligence Risk Management Framework (AI RMF 1.0)

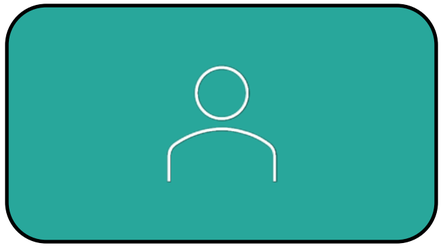
Data privacy is particularly important for nonprofits, who often have access to sensitive information from the public

Financial Information

Health Records

Housing Conditions

Carceral Status



Other Personal Histories

But even when nonprofits aren't privy to the above, they still must safeguard data provided by employees, donors, volunteers and other information.

Privacy stewards are responsible for a few key functions

Responsibilities

Ensuring AI compliance and privacy

Supporting privacy functions for contracts and partnerships

Creating Data Access Guidelines for:
- Manual Access
- Programmatic Access

Facilitating data privacy for users in a CRM

Potential Titles

IBM's resource on AI in business delves into the function of the Chief privacy office on page 13

Keep the privacy principles of anonymity, control, and confidentiality top of mind when designing and developing AI Systems

Anonymity:
When possible, limit PII

Control:
Maintain control over training AI models with nonprofit content

Confidentiality:
Abide by key confidentiality policies and seek consent

NIST has long been a leader in the privacy domain. Their values are excerpted and adapted for the nonprofit use case from from pg. 17 of their Artificial Intelligence Risk Management Framework (AI RMF 1.0)

For Tech Builders: Additional privacy-enhancing technology considerations can support effective AI implementation

Data sparsity can reduce accuracy of privacy techniques

De-identification, aggregation, and privacy-enhancing technologies support privacy-focused AI systems

Example

mRelief SNAP Eligibility Check

They use de-identification techniques to help people check their eligibility for SNAP with roughly ten simple questions that limit requests for personal information to one PII question (phone number), which is optional.

NIST has long been a leader in the privacy domain. Their section on PET considerations are excerpted from pg. 17 and adapted for the nonprofit use case from their Artificial Intelligence Risk Management Framework (AI RMF 1.0)

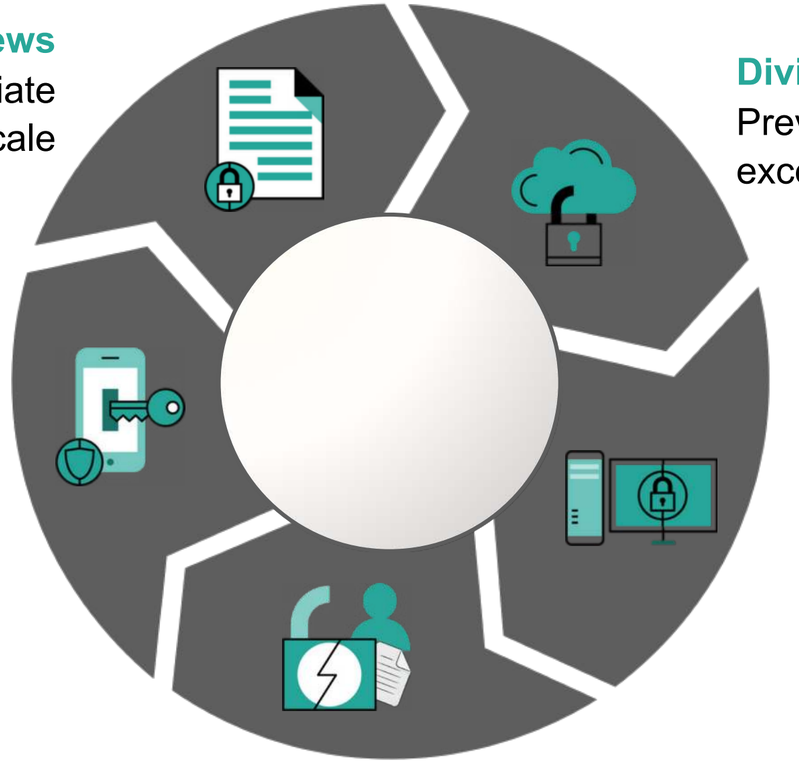
Enhance privacy by considering these steps on data access & permissions

- Review organizational documentation that governs privacy with AI in mind
- Create a section of your Privacy Policy or Terms of Use that focuses on AI with key practices in mind
- Revisit the impact of AI on confidentiality clauses for employees and participants (if a direct service organization) to ensure they are comprehensive to support privacy enhanced AI systems

Mitigating risk is the foundation of strong privacy practices

Regular Reviews
Ensures permissions remain appropriate as you scale

Division of Duties
Prevents one person from having excessive control



Multi-factor Authentication
Reduces the risks of unauthorized users

Principle of Least Privilege**
Grants users the minimum permissions necessary

Principle of Minimization
Decreases workload and lessens likelihood information will be vulnerable in a breach

*FrontEgg focuses on securing end-users access experience through granular, multi-tenant authentication. They have written about MFA, Principles of Least Privilege and Regular Reviews here and we have excerpted this above for the nonprofit use case **Cloud Security Alliance (CSA) is a not-for-profit organization with the mission to "promote the use of best practices for providing security assurance within cloud computing, and to provide education on the uses of cloud computing to help secure all other forms of computing. They have written at length about Just In Time Privilege and its relationship with the principle of least privilege which we incorporate in the definition above and present here for a learning resource

THANK YOU!

https://www.anbadvisory.com/