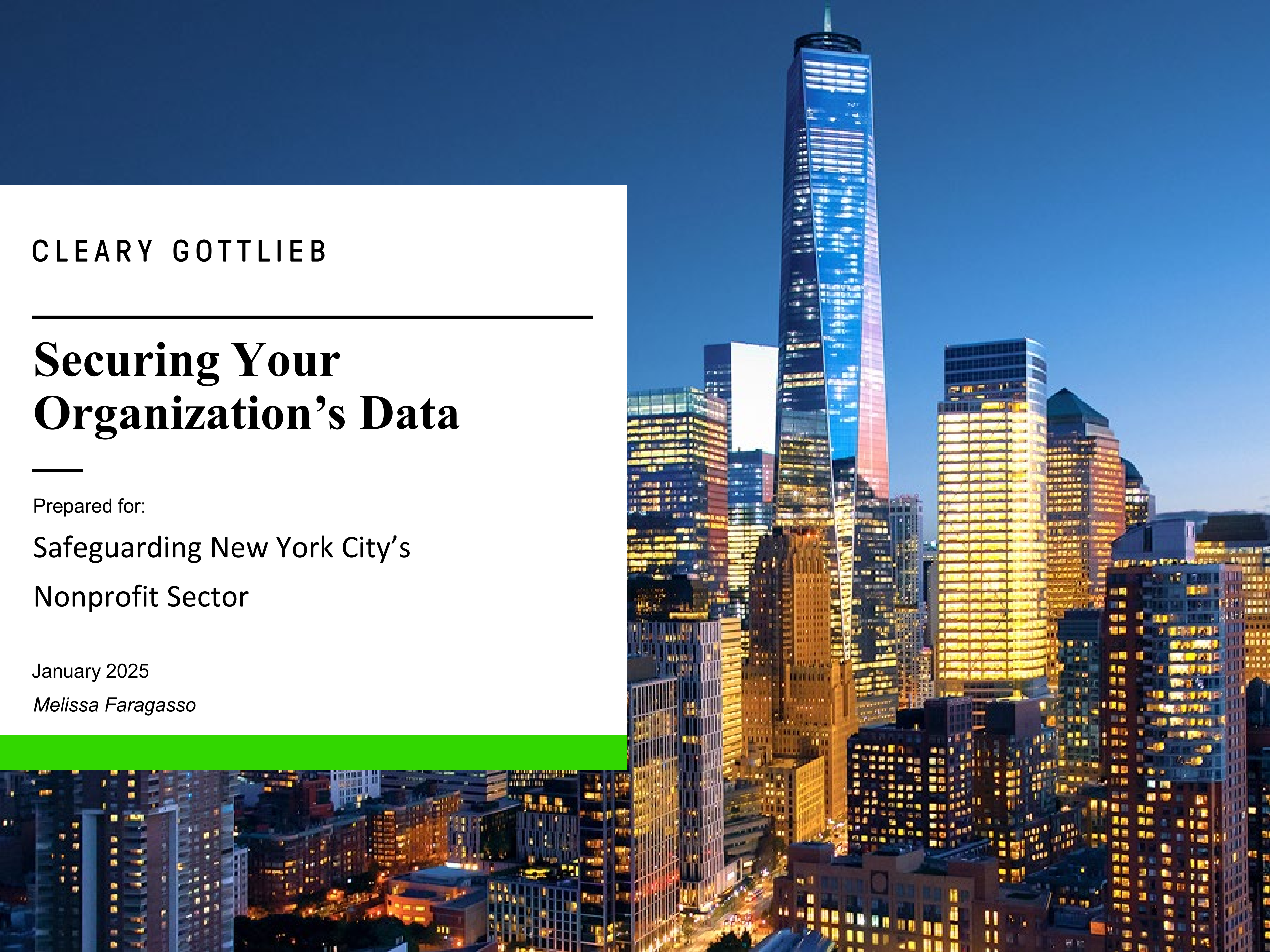


CLEARY GOTTLIEB

Securing Your Organization’s Data

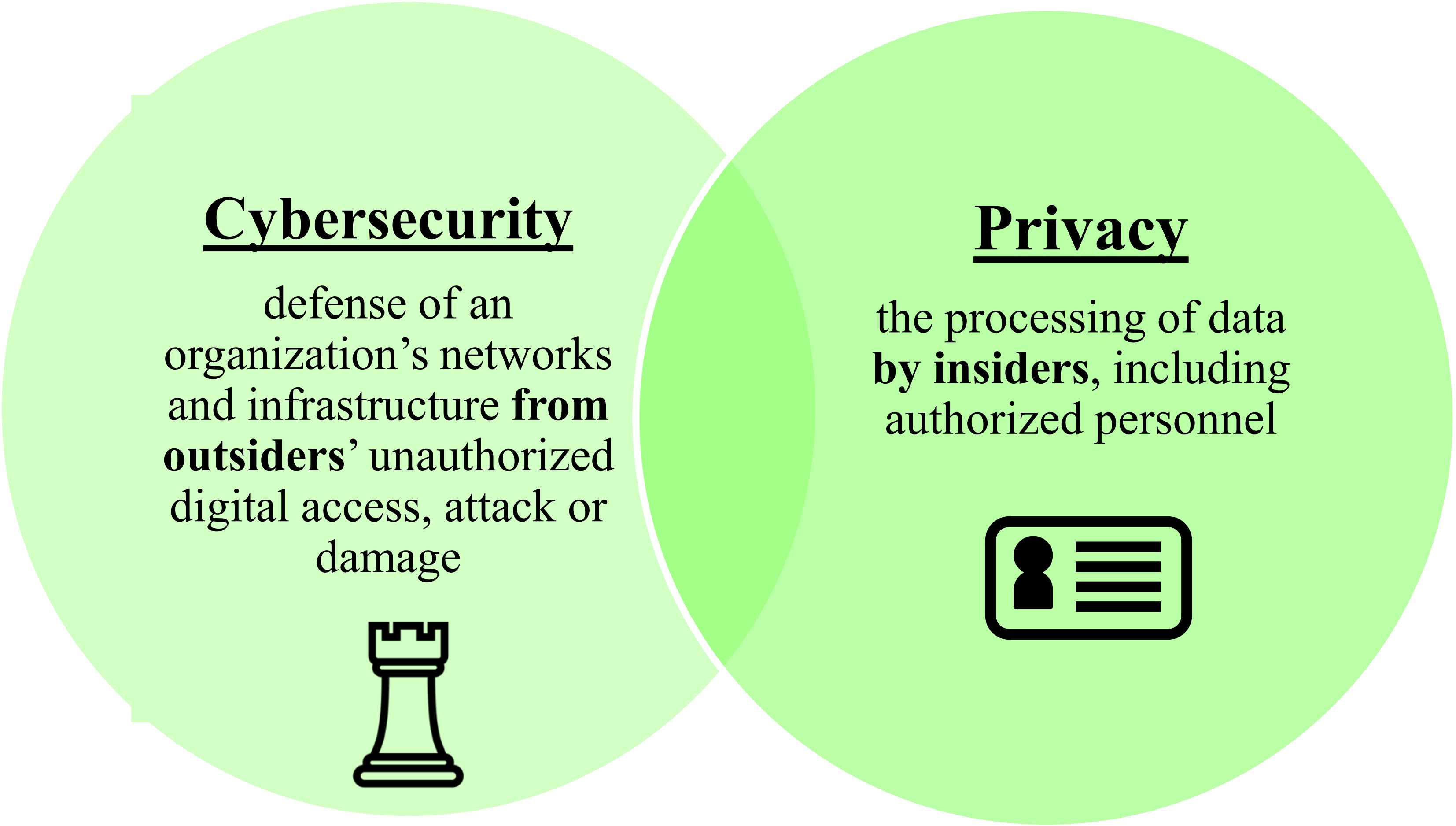
Prepared for:

Safeguarding New York City’s Nonprofit Sector

January 2025

Melissa Faragasso

Cybersecurity and Privacy Are Related Concepts



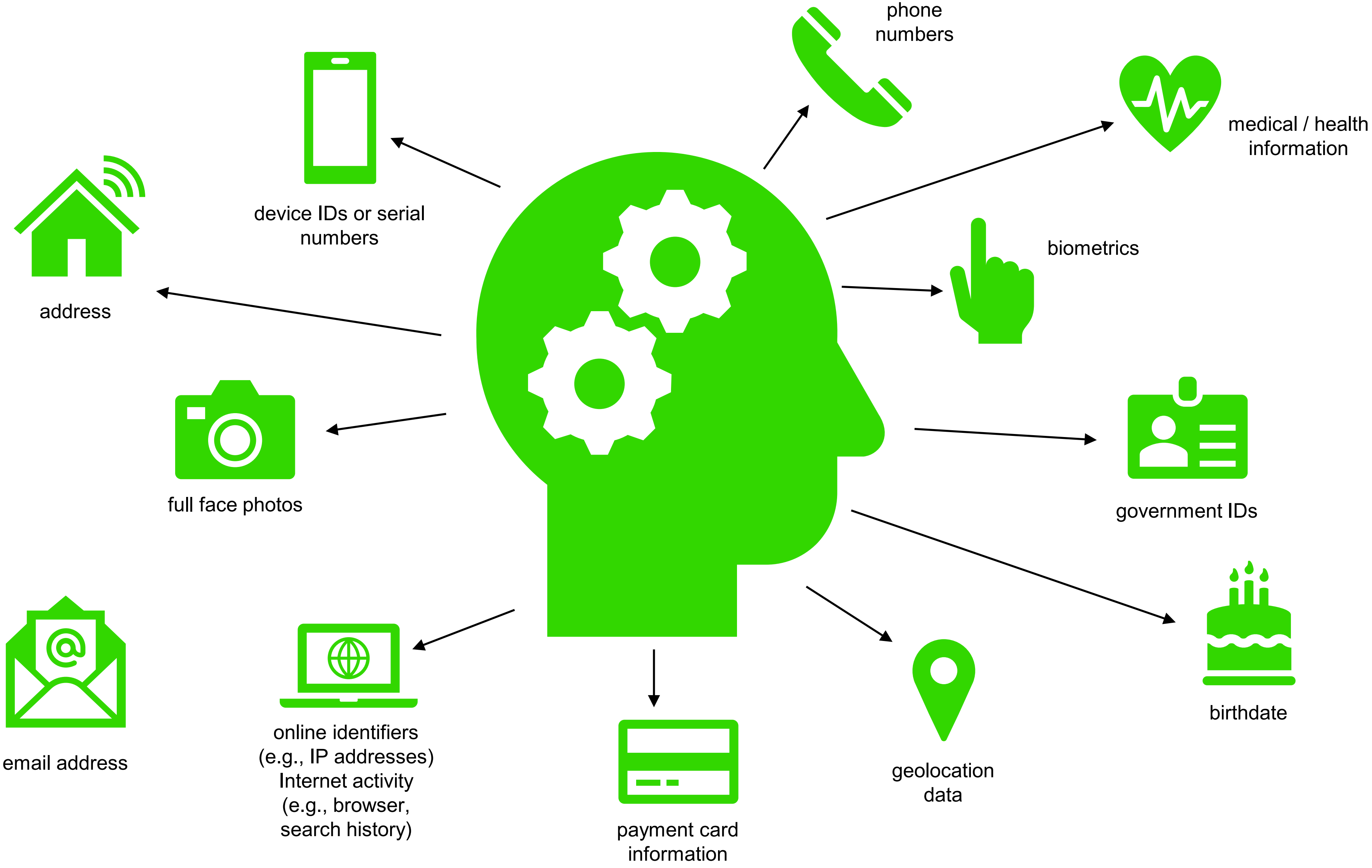
Cybersecurity

defense of an organization’s networks and infrastructure **from outsiders**’ unauthorized digital access, attack or damage

Privacy

the processing of data **by insiders**, including authorized personnel

What is "Personal Data"?



phone numbers

medical / health information

device IDs or serial numbers

address

biometrics

full face photos

government IDs

email address

online identifiers (e.g., IP addresses) Internet activity (e.g., browser, search history)

payment card information

geolocation data

birthdate

Overview of Generally Applicable Data Protection Principles

Lawfulness, Fairness and Transparency

Purpose Limitation

Data Minimization

Accuracy

Storage Limitation

Integrity and Confidentiality

Accountability

Data Subject Rights Requests

Data Protection Best Practices

1. **Develop data maps and inventories** to track what personal data is collected, for what purpose it is collected and to whom it is disclosed

2. **Employ data minimization** by collecting, processing and retaining only the personal data necessary for the intended purpose, and ensure such data collected is proportionate to that purpose

3. **Avoid collection of sensitive data (e.g., geolocation data, health data, children's data)** unless specifically necessary for the processing purpose, and subjected to heightened protections

4. **Develop internal data protection policies and procedures**, such as data retention and incident response policies, as well as policies and procedures to **respond to and comply with state agencies and subpoena requests**

5. **Delete or, with respect to personal data, anonymize, aggregate or deidentify data** that the organization no longer needs to retain unless otherwise required by law

6. **Review contracts with state and federal agencies** to determine data protection obligations and use restrictions

7. **Conduct diligence of, and continuously audit and monitor, third party vendors** with whom confidential data is shared to ensure appropriate usage of data and to protect against misuse

8. **Educate and train employees and volunteers** on appropriate handling and usage of confidential and personal data, including how to respond in the event of a data breach or other security incident

9. **Implement robust data security and access controls**, including (i) use of strong passwords and multi-factor authentication and (ii) physical and electronic access controls to safeguard data from unauthorized access or disclosure

10. **Take steps to protect against Internet scams**, such as phishing or other AI-enabled social engineering attempts, such as by implementing access controls and training employees to recognize and report such incidents

CLEARY GOTTLIEB STEEN & HAMILTON LLP

clearygottlieb.com

Throughout this presentation, “Cleary Gottlieb” and the “firm” refer to Cleary Gottlieb Steen & Hamilton LLP
and its affiliated entities in certain jurisdictions, and the term “offices” includes offices of those affiliated entities.