Privacy Training

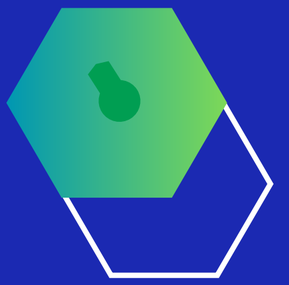
Olivia Criscione

1A. What is Privacy?

- The primary element of cybersecurity is privacy, which is the assurance that private data is shielded from unwanted access, manipulation, or distribution.
- In today's digital world, maintaining privacy is crucial since personal information is constantly being created, shared, and stored via the internet.
- The surge in cyber threats, such as data breaches, identity theft, and hacking, highlights the significance of rigorous privacy measures and regulations.

1B. What is Privacy?

- Safeguarding privacy upholds personal freedoms by guaranteeing the confidentiality of sensitive information including financial and personal data.
  - This creates trust in the digital world for users
- Ensuring that only those individuals have access to sensitive information for valid reasons is essential in order to lower the risk of data breaches and unapproved disclosures.

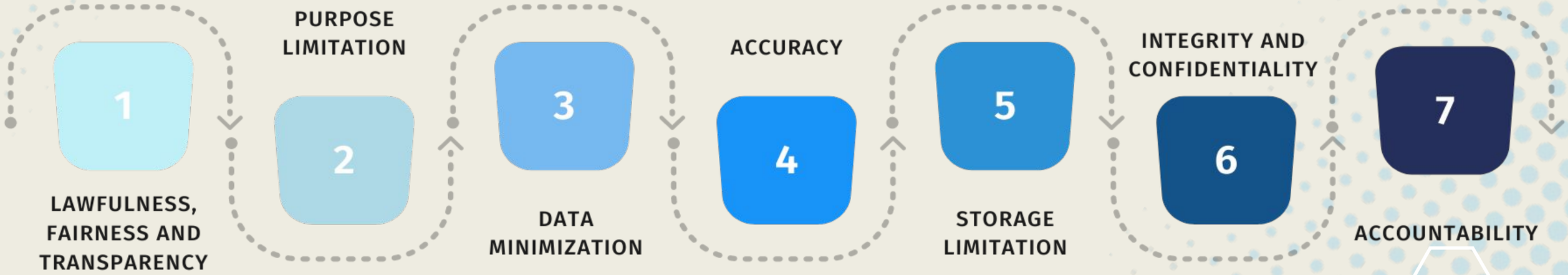


2. What is Business Privacy?

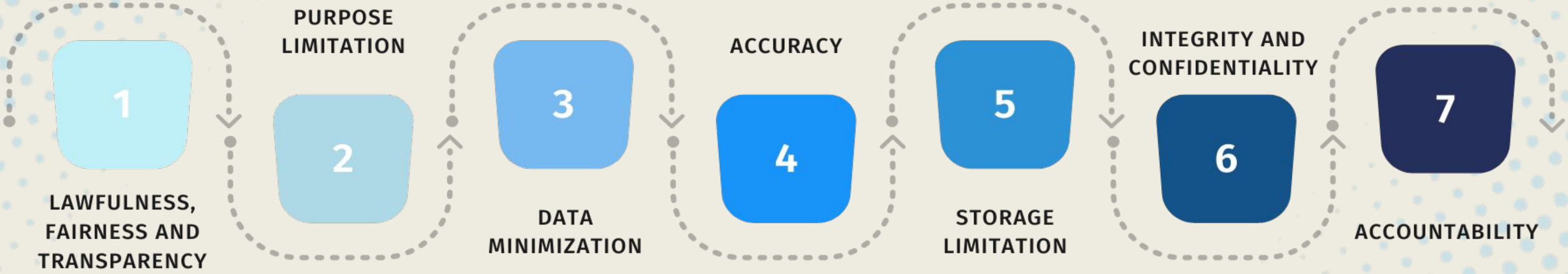
- Business Privacy is the protection of sensitive information and data owned or handled by a business entity from unauthorized access, disclosure, alteration, or destruction.
- Preserving business data privacy helps to build user, client, and customer trust—a critical component of any company's reputation.
- Organizations can employ encryption techniques, access limits, and frequent security audits to guarantee data privacy.

3A. Generally Accepted Privacy Principles

- Regulations comparable to the General Data Protection Regulation (GDPR) in Europe and other similar laws around the world specify how businesses must manage and safeguard personal data. Consent requirements, data breach reporting obligations, and user rights are included.
- GDPR is split into seven different aspects:

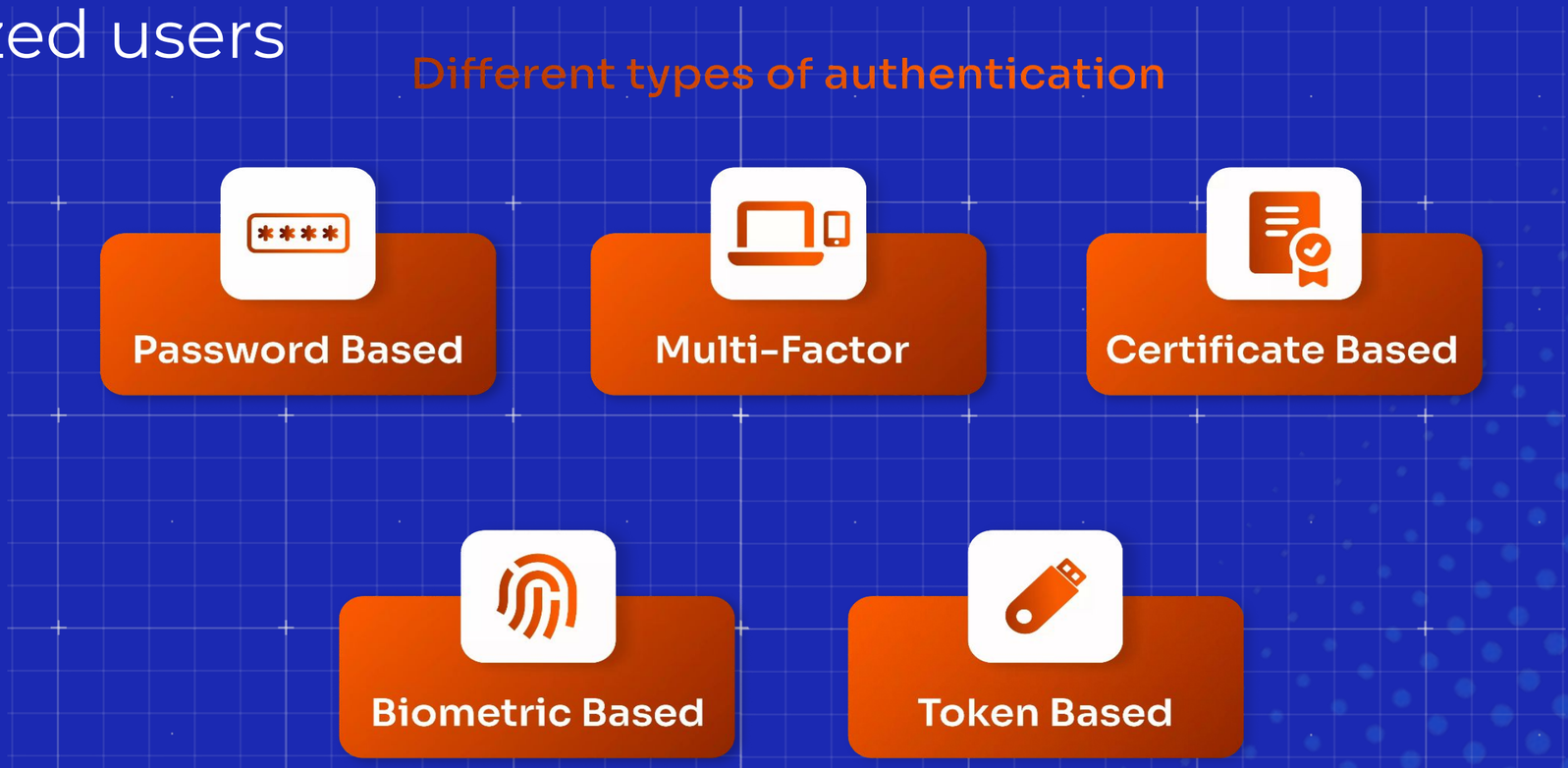


3B. General Data Protection Regulations (GDPR)



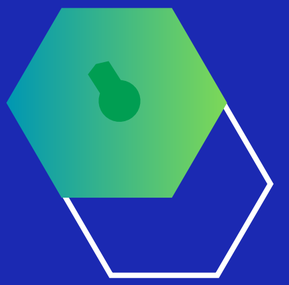
4. Authentication

- Is the process of verifying the identity of users
  - Examples of authentication processes include: usernames, passwords, biometrics, or two factor authentication / multi-factor authentication.
- Authentication processes help to protect systems from unauthorized users



5. Identity vs. Anonymity

- Identity is associating actions with specific individuals or users.
  - Allows online activities of users to be traceable for accountability purposes.
- Anonymity is the concealing of individuals identities
  - Prevents the identification of certain users involved in certain digital activities and transaction in order to preserve privacy and confidentiality.
- The balance of identity vs. anonymity
  - Balance between identifying individuals for accountability while also maintaining their right to privacy and anonymity is important.



6. Anonymity

- Anonymity is:
  - Protecting personal information
    - Shielding users' identities and personal details from being revealed or linked to specific digital actions or behaviors.
  - Ensuring privacy in data collection
  - Ensuring privacy in data processing
    - Using anonymity techniques and minimizing data linkage is possible by replacing identifying information with other identifiers.

7. Protection Measures

- Encryption of Data
  - Is the process of converting plaintext data into ciphertext using cryptography to prevent unauthorized access or interception of sensitive information.
- Security Audit / Assessment Schedules
  - Conducting audits of of security controls, systems, and processes on a regular basis.
- Employee Trainings
  - Providing detailed education and training programs to staff members on security best practices, privacy regulations, and methods for protecting sensitive data.

8. Organizational training for users

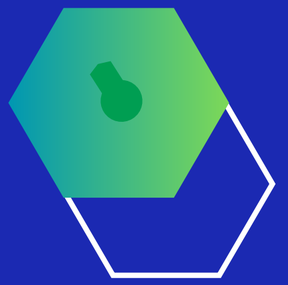
- Educating users about the value of privacy, their rights and obligations, and the safest ways to handle sensitive data.
- Offering guidance on how to manage, preserve, send, and dispose of private information in a secure manner to reduce the possibility of privacy violations.
- Ensuring that employees understand and comply with relevant privacy laws, regulations, and industry standards applicable to their roles and responsibilities by providing them with trainings on industry requirements.

9. What is the purpose of privacy and why is it implemented?

- The purpose is to protect personal / sensitive information:
  - Privacy safeguards sensitive data like financial records and medical history from unauthorized access and identity theft.
- It is implemented to maintain trust and compliance
  - Privacy policies and procedures help foster trust between individuals and companies by preserving confidentiality and integrity of sensitive information.
  - It also helps protect companies proprietary information from being manipulated or stolen.

Conclusion

- Privacy policies and procedures help protect both organizations and people.
- Following policy policies within organizations helps in creating and maintaining customer confidence and trust with an organization.
- The proper privacy training will help in maintaining customer trust while also creating confidence within the organization in relation to keeping sensitive data private.
- Privacy is the driver behind the cyber security industry.
  - The main concept of cyber security is to safeguard sensitive information from individuals who are unauthorized to view that information.



References:

- https://csrc.nist.gov/glossary/term/privacy
- https://www.cyberark.com/resources/blog/data-privacy-day-data-protection-lessons-from-the-2010s
- https://csrc.nist.gov/glossary/term/privacy
- https://dataprivacymanager.net/what-are-the-7-gdpr-principles/
- https://www.miniorange.com/blog/different-types-of-authentication-methods-for-security/