Ethical and Legal Considerations in Data Scienc

Unit 8

Data Privacy and Security

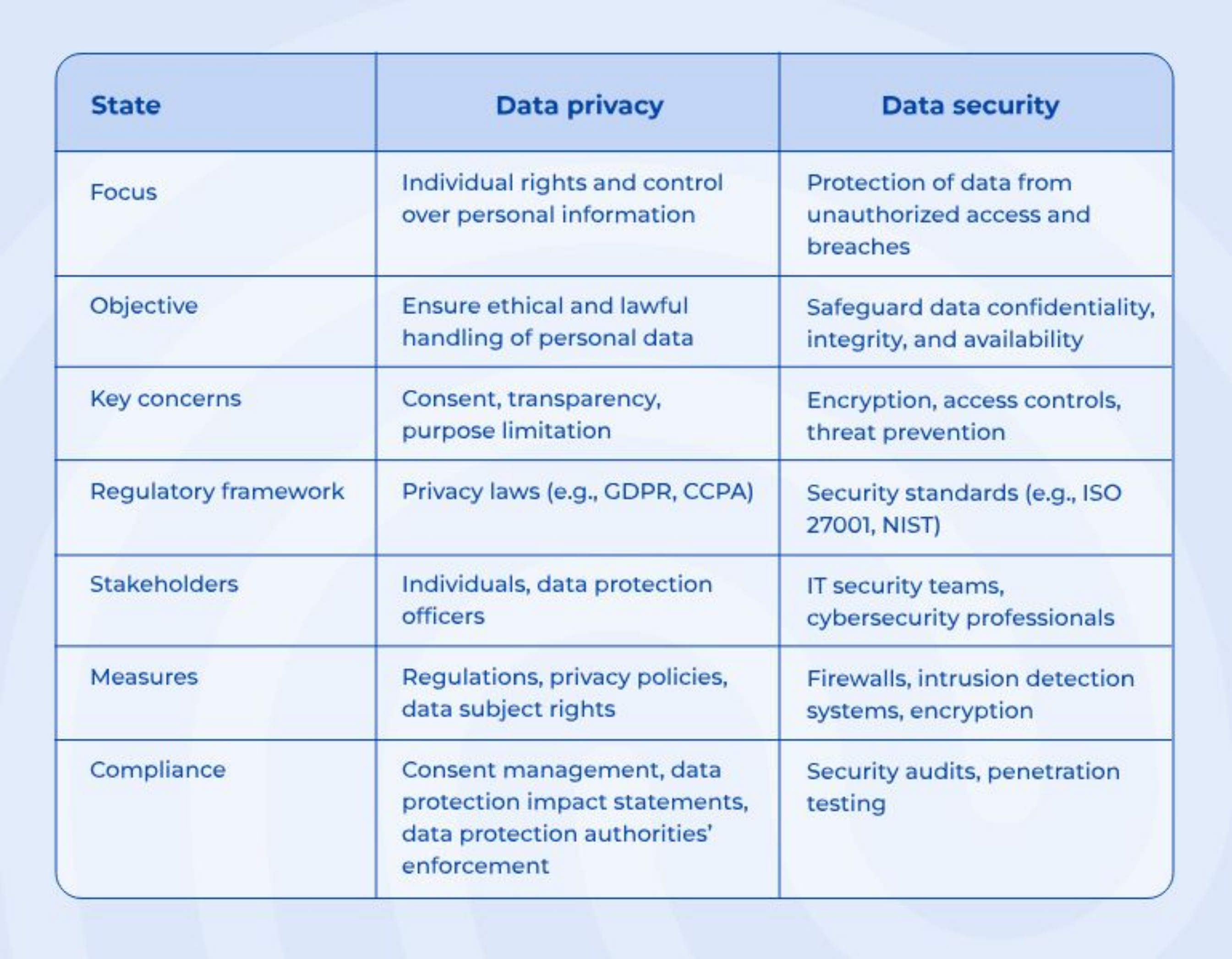
Data privacy refers to the proper handling, processing, storage, and usage of personal information.

It focuses on ensuring that sensitive data, such as names, addresses, and financial information, is managed responsibly and with consent from the data subjects

Data security involves protecting digital information from unauthorized access, theft, corruption, or exploitation throughout its lifecycle. It ensures data integrity, availability, and confidentiality

Data Privacy and Security

Data privacy focuses on the rights and consent of individuals regarding their personal data, while data security provides the technical measures to protect that data



State	Data privacy	Data security
Focus	Individual rights and control over personal information	Protection of data from unauthorized access and breaches
Objective	Ensure ethical and lawful handling of personal data	Safeguard data confidentiality, integrity, and availability
Key concerns	Consent, transparency, purpose limitation	Encryption, access controls, threat prevention
Regulatory framework	Privacy laws (e.g., GDPR, CCPA)	Security standards (e.g., ISO 27001, NIST)
Stakeholders	Individuals, data protection officers	IT security teams, cybersecurity professionals
Measures	Regulations, privacy policies, data subject rights	Firewalls, intrusion detection systems, encryption
Compliance	Consent management, data protection impact statements, data protection authorities' enforcement	Security audits, penetration testing

Ethical and Legal Considerations in Data Science

Bias in data science refers to the systematic errors or distortions in data collection, analysis, or model outputs that can lead to unfair or discriminatory outcomes.

Bias can perpetuate existing social disparities and undermine fairness in decision-making processes

To remove biasness, Regular data audits must be maintained to identify biases, use of fairness-aware algorithms, ensure diverse representation in datasets

Ethical and Legal Considerations in Data Science

Transparency involves being open about data sources, methodologies, and model outputs to ensure that stakeholders understand how decisions are made.

Lack of transparency can lead to mistrust and make it difficult to identify biases or errors in decision-making processes

To handle transparency, Clear documentation of data sources and methodologies must be done, Providing explanations for model outputs and decisions

Ethical and Legal Considerations in Data Science

Accountability refers to the responsibility of data scientists and organizations to ensure that their practices are ethical and that they are answerable for any negative consequences of their work.

Ensures that individuals or entities are held responsible for any harm caused by data-driven decisions

Handling Ethical Issues in Data Science

- Follow established codes of conduct and ethical standards that guide data science practices, ensuring accountability and transparency
- Ensure that data collection and usage respect individuals' privacy rights, obtaining informed consent when necessary
- Use fairness-aware algorithms and techniques to reduce bias in models, ensuring they do not unfairly disadvantage certain groups
- Maintain clear documentation of design processes and decision-making to ensure transparency
- Hold themselves and others accountable for the impact of their work
- Stay updated on ethical considerations and emerging technologies
- Engage with diverse stakeholders, including ethicists and legal experts, to ensure that data science projects are ethically sound
- Use ethical assessment checkpoints and seek independent advice to manage ethical risks

Legal Considerations: Data Protection Laws, Intellectual Property

Data protection laws and intellectual property rights are crucial considerations in data science, as they impact how data is collected, processed, and used

Data scientists must ensure that their practices comply with data protection laws, obtaining necessary consents and minimizing data collection

Implement robust security measures, anonymize data when possible, and limit access to sensitive information

Ensure that scientific research respects privacy laws while providing meaningful protections for personal information

Current scenario of data laws in Nepal

The Individual Privacy Act, 2018, protects personal information, but lacks comprehensive rights like data portability and erasure.

The Data Act 2079 aims to streamline data management but needs clearer guidelines on data minimization.

The Individual Privacy Act emphasizes consent but lacks detailed provisions for transparency.

Nepal's Current Framework ‘The National Penal Code’ and ‘Data Act 2079’ address some aspects of data security but lack specific breach notification requirements.

Nepal's Current Framework currently lacks a specific data protection authority, relying on courts for enforcement.

The Data Act 2079 does not address extra-territorial applicability clearly.

The Individual Privacy Act provides for fines and imprisonment but may need more specific penalties for data protection violations.