Implications of AI on Privacy and Security through a Data Lens

Sanjeev Gathani

Table of Content

- Handling Personal Data
- Security of Personal and Business Data
- Definitions
- Introduction
- Guiding principles
- Framework components
- Risks and governance

11 STEPS TO SAFE HANDLING OF PERSONAL DATA

1 COLLECT FOR A PURPOSE

Collect only the Personal Data that is required for the specified purpose(s).

2 NOTIFY THE DATA SUBJECT

Ensure that the resident/public is clearly notified of the purpose for Personal Data collection and is given an option to opt-out.

3 GET CONSENT

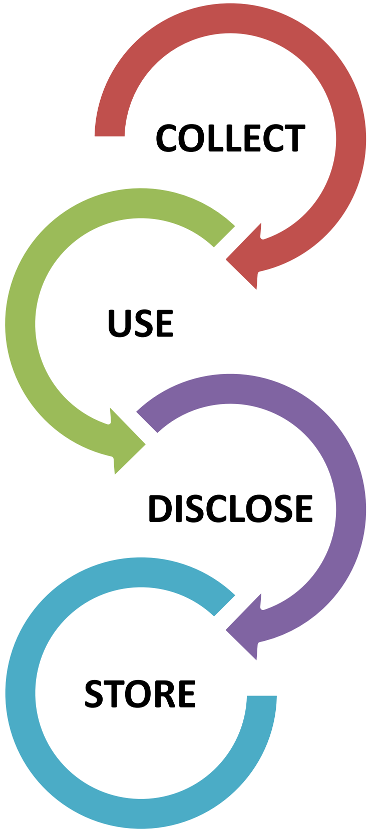
Get consent to use the data for the notified purposes. Get explicit consent for 3rd party sharing of the data. Keep records of evidence of consent.

4 ENSURE DATA IS ACCURATE

Ensure accuracy through integrity of processes that maintain Personal Data.

5 ACCESS & CORRECTION RIGHTS

Data subjects have rights to access and correct their Personal Data held by the organisation.



6 PROTECT PERSONAL DATA

Personal Data must be secured from unauthorised use and access

7 LIMIT UNNECESSARY RETENTION

Personal Data should not be retained once its purpose has been fulfilled.

8 SECURE OVERSEAS TRANSFERS

Personal Data moved out of Singapore must be supported and secured with necessary documentation.

9 SUPPORT DATA PORTABILITY

Allow individuals to transfer their personal data under your care to another organisation

10 MANAGE DATA BREACH

Notify the PDPC and affected individuals of 'significant' data breaches

11 TIMELY HANDLING OF COMPLAINTS AND ENQUIRIES

Ensure that enquiries and complaints regarding the handling of Personal Data is directed to the DPO Team.

10 MORE STEPS TO ENSURE SECURITY OF PERSONAL & BUSINESS DATA

1 ACCESS LIMITATION

Access to personal data should only be granted to those who need it to perform their job

2 CONFIDENTIALITY & NON-DISCLOSURE AGREEMENT

All employees are bound to protect the confidentiality of personal data they handle.

3 USE OF OFFICE EQUIPMENT

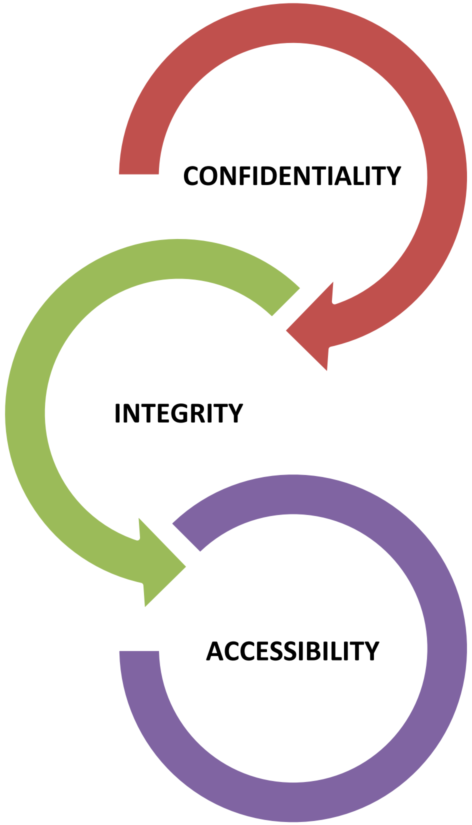
Ensure that personal data is not left unattended on printers and copiers. Onboard storage devices must be secured before leased equipment is returned.

4 MOVEMENT OF CONFIDENTIAL DOCUMENTS

Proper protocol includes the use of tamper proof or lockable cases, a handover & acknowledgement process.

5 SERVICE COUNTERS

All files/paper documents/in-trays at the service counter should be shielded from public view and lockable storage used where necessary. Must have a process for handover and receipt of files and documents.



6 STAFF WORKSPACE

All staff should adopt a clean-desk policy. Offices and computers should be locked when unattended.

7 HARDWARE & SOFTWARE INSTALLATION, MODIFICATION & REMOVAL

Only authorised personnel are permitted to add, remove or modify any equipment, hardware or software within the organisation’s environment.

8 SOCIAL MEDIA

Never comment on anything related to legal matters and remember that whatever you publish is widely accessible and can be traced back to the organisation.

9 MOBILE DEVICES

Immediately report loss or theft to the IT Service Desk or local IT.

10 EXTERNAL STORAGE MEDIA

Only storage media issued by the organisation may be used.

Definitions

Information (typically held electronically) about a particular person, especially sensitive information regarding their finances, medical history, etc

Personal data, also known as personal information or personally identifiable information (PII), is any information related to an identifiable person

Personal data is defined under the GDPR as "any information which [is] related to an identified or identifiable natural person". The IP address of an Internet subscriber may be classed as personal data.

Definitions

- Artificial intelligence (AI) is the theory and development of computer systems capable of performing tasks that historically required human intelligence, such as recognizing speech, making decisions, and identifying patterns

Definitions

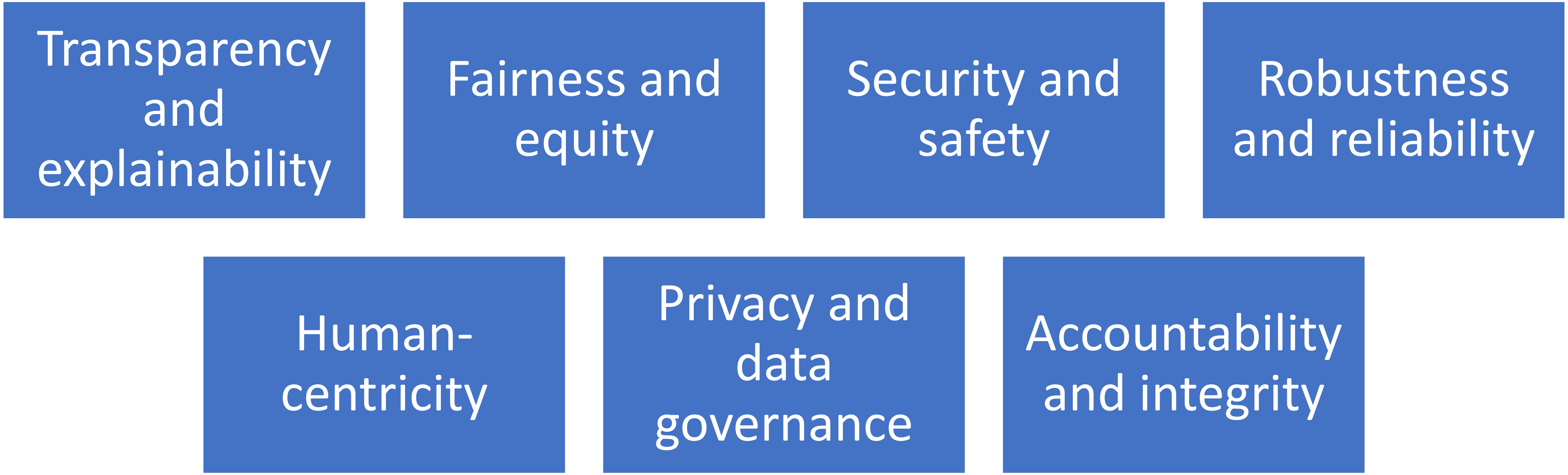
Broadly speaking, privacy is the right to be let alone, or freedom from interference or intrusion. Information privacy is the right to have some control over how your personal information is collected and used

Security is the quality or state of being secure, such as freedom from danger, fear, or anxiety

Introduction

- A practical guide for organizations that wish to design, develop and deploy traditional AI technologies in commercial and non-military or dual use applications

Guiding Principles



- Transparency and explainability
- Fairness and equity
- Security and safety
- Robustness and reliability
- Human-centricity
- Privacy and data governance
- Accountability and integrity

Transparency and Explainability

- Transparency refers to providing disclosure on when an AI system is being used and the involvement of an AI system in decision-making, what kind of data it uses, and its purpose. By disclosing to individuals that AI is used in the system, individuals will become aware and can make an informed choice of whether to use the AI enabled system.
- Explainability is the ability to communicate the reasoning behind an AI system's decision in a way that is understandable to a range of people, as it is not always clear how an AI system has arrived at a conclusion.
- This allows individuals to know the factors contributing to the AI system's recommendation.
- In order to build public trust in AI, it is important to ensure that users are aware of the use of AI technology and understand how information from their interaction is used and how the AI system makes its decisions using the information provided.

Fairness and Equity

- Deployers should have safeguards in place to ensure that algorithmic decisions do not further exacerbate or amplify existing discriminatory or unjust impacts across different demographics and the design, development, and deployment of AI systems should not result in unfair biasness or discrimination.

Security and Safety

AI systems should be safe and sufficiently secure against malicious attacks.

Safety refers to ensuring the safety of developers, deployers, and users of AI systems by conducting impact or risk assessments and ensuring that known risks have been identified and mitigated.

A risk prevention approach should be adopted, and precautions should be put in place so that humans can intervene to prevent harm, or the system can safely disengage itself in the event an AI system makes unsafe decisions - autonomous vehicles that cause injury to pedestrians are an illustration of this.

Ensuring that AI systems are safe is essential to fostering public trust in AI.

Human-Centricity

AI systems should respect human-centred values and pursue benefits for human society, including human beings’ well-being, nutrition, happiness, etc.

It is key to ensure that people benefit from AI design, development, and deployment while being protected from potential harms. AI systems should be used to promote human well-being and ensure benefit for all.

Especially in instances where AI systems are used to make decisions about humans or aid them, it is imperative that these systems are designed with human benefit in mind and do not take advantage of vulnerable individuals.

Privacy and Governance

AI systems should have proper mechanisms in place to ensure data privacy and protection and maintain and protect the quality and integrity of data throughout their entire lifecycle. Data protocols need to be set up to govern who can access data and when data can be accessed.

Data privacy and protection should be respected and upheld during the design, development, and deployment of AI systems. The way data is collected, stored, generated, and deleted throughout the AI system lifecycle must comply with applicable data protection laws, data governance legislation, and ethical principles.

Accountability and Integrity

There needs to be human accountability and control in the design, development, and deployment of AI systems.

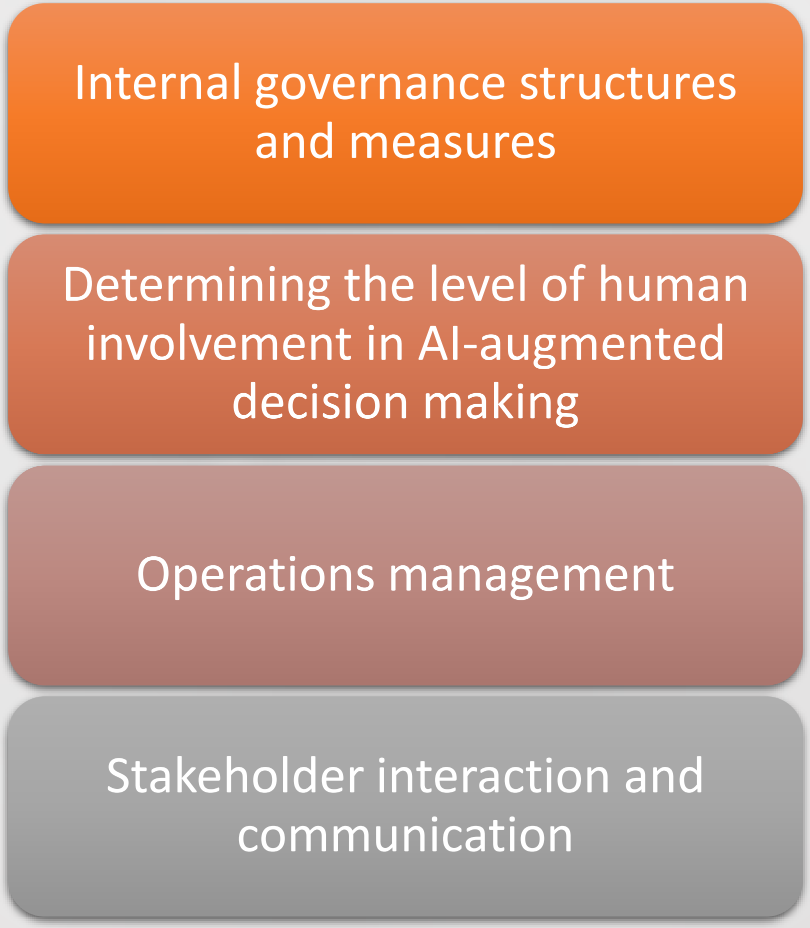
Deployers should be accountable for decisions made by AI systems and for the compliance with applicable laws and respect for AI ethics and principles. AI actors should act with integrity throughout the AI system lifecycle when designing, developing, and deploying AI systems.

Robustness and Reliability

AI systems should be sufficiently robust to cope with errors during execution and unexpected or erroneous input, or cope with stressful environmental conditions. It should also perform consistently. AI systems should, where possible, work reliably and have consistent results for a range of inputs and situations.

AI systems may have to operate in real-world, dynamic conditions where input signals and conditions change quickly. To prevent harm, AI systems need to be resilient to unexpected data inputs, not exhibit dangerous behaviour, and continue to perform according to the intended purpose.

Key Components



Internal governance structures and measures

Determining the level of human involvement in AI-augmented decision making

Operations management

Stakeholder interaction and communication

Governance of Generative AI

Risks include:

- Deepfakes, impersonation, fraudulent and malicious activities
- Privacy and confidentiality
- Propagation of embedded biases
- Factually inaccurate responses and disinformation
- Infringement of intellectual property rights

Governance of Generative AI

Governance should include:

- Manage the risks of generative AI
- How to distinguish between AI-generated content versus authentically generated ones

Questions and Answers

Thank You