Artificial Intelligence (AI) Business considerations

Rail Delivery Group

National Rail

Alan Cain
Chief Information Security Officer

Introduction:

As businesses increasingly incorporate Artificial Intelligence (AI) into their operations, the potential risks to data security, particularly regarding personally identifiable information (PII), cannot be ignored. This document serves as a comprehensive guide, outlining essential measures and best practices to safeguard against these risks. It is designed to assist organisations in aligning their AI strategies with the stringent requirements of the Data Protection Act 2018 and GDPR, ensuring a balance between innovation and data privacy. Our goal is to provide actionable insights that enable businesses to harness the power of AI while maintaining the highest standards of data protection.

Key Considerations:

Data Protection by Design and Default:
Under GDPR, which is incorporated into UK law by the Data Protection Act 2018, organisations are required to implement data protection principles from the onset of designing systems. This includes ensuring that personal data is processed securely, lawfully, and in a manner that protects against unauthorised or unlawful processing, accidental loss, destruction, or damage.

Data Models:
When using artificial intelligence (AI) models for processing business-sensitive information or in scenarios where there is a potential for Personally Identifiable Information (PII) to be involved, it is prudent to consider the deployment of private models over public ones, particularly from an intellectual property (IP) perspective.

Private models are hosted within a controlled environment, ensuring that sensitive data remains within the confines of the organisation's infrastructure. This mitigates the risk of unintentional data exposure or breaches, which can be more prevalent in public model settings where data might transit through or be stored in external servers.

Contract Clauses:
When employing artificial intelligence to develop software or applications, it is crucial to incorporate specific clauses in the contract. These clauses must guarantee that the business retains ownership of the generated code, rather than any external party, and that the code cannot be repurposed for use with other clients.

Data Minimisation:
Limit the collection of PII to what is strictly necessary for the intended purpose. AI systems should be designed to process only the data needed for their tasks, reducing the risk of exposure in the event of a breach.

Alan Cain
Chief Information Security Officer

Transparency:
Ensure transparency in AI operations, allowing individuals to understand how their data is used and processed. This aligns with the GDPR's principle of fairness and transparency.

User Consent:
Where applicable, obtain explicit consent from individuals for processing their PII, ensuring that consent is informed, specific, and freely given. This is particularly relevant when AI is used in new or unexpected ways that individuals might not anticipate.

Risk Assessment:
Conduct thorough risk assessments to identify potential vulnerabilities within AI systems that could lead to PII exposure. This should involve evaluating the AI's data processing and storage mechanisms, and the security measures in place to protect against cyber threats.

Encryption and Anonymisation:
Implementing strong encryption for stored and transmitted data can significantly reduce the risk of unauthorised access. Where possible, consider anonymising data so that the individuals cannot be identified, thereby reducing the risks associated with data processing.

Access Controls:
Ensure strict access controls are in place for systems processing PII. This includes limiting access to those who need it for their role, employing multi-factor authentication, and regularly reviewing access permissions and logs.

Regular Audits and Monitoring:
Regularly audit AI systems for compliance with data protection laws and conduct continuous monitoring to detect and respond to security incidents promptly.

Incident Response Plan:
Develop and maintain an effective incident response plan that includes procedures for responding to data breaches. This should align with the GDPR requirement to report certain types of personal data breaches to the relevant supervisory authority within 72 hours of becoming aware of the breach.

Staff Training:
Ensure staff are trained in data protection and understand the risks associated with AI systems. This includes training on recognising and responding to cyber threats.

Data Protection Impact Assessments (DPIAs):
Conduct DPIAs for AI projects, as recommended by GDPR, to assess privacy risks systematically and comprehensively to individuals in the context of the proposed processing.

Simplification for Broader Understanding:
Think of AI in the business like a highly efficient but potentially risky employee. Just as you would ensure an employee understands company policies and procedures to protect sensitive information, you need to design AI systems with built-in safeguards (***Data Protection by Design and Default***).

Alan Cain
Chief Information Security Officer

Regularly check for any gaps in the system's security (***Risk Assessment***) and keep all sensitive information locked in a safe (***Encryption***) that only a few trusted people can access (***Access Controls***). Keep an eye on the system (***Regular Audits and Monitoring***) and have a plan ready for what to do if something goes wrong (***Incident Response Plan***). Make sure everyone in the company knows the importance of keeping data safe and how to do it (***Staff Training***). Before you launch any new AI project, make sure it is not going to put people's privacy at risk (***DPIAs***).

It is about being proactive, cautious, and responsible when integrating AI into your business operations to protect users' personal information from potential risks.

Alan Cain
Chief Information Security Officer