

Data Protection Impact Assessment (DPIA)

Be Data Solutions Limited

1. Introduction

This Data Protection Impact Assessment (DPIA) is conducted to evaluate and mitigate data protection and privacy risks associated with the data and software services provided by Be Data Solutions. This assessment ensures that all data processing activities comply with relevant data protection regulations, such as the General Data Protection Regulation (GDPR), and safeguards individuals' privacy.

2. Purpose of the DPIA

The purpose of this DPIA is to:

- Identify and assess risks related to the data processing activities.
- Evaluate the potential impact on individuals' privacy.
- Implement measures to address identified risks.
- Ensure compliance with data protection laws.

3. Description of Services

3.1 Data Services

- **Data Strategy:** Developing strategic approaches for managing and utilizing data to enhance decision-making and business outcomes.
- **Data Engineering:** Designing, building, and maintaining data pipelines and architectures to ensure efficient data storage, retrieval, and processing.
- **Data Analytics:** Analyzing large datasets to provide actionable insights and support informed decision-making.
- **Data Science:** Utilizing scientific methods, algorithms, and systems to extract knowledge and insights from structured and unstructured data.
- **Machine Learning:** Applying algorithms and models that enable systems to learn from data and make predictions or decisions without explicit programming.

3.2 Software Services

- **Software Development:** Creating and maintaining custom software solutions tailored to client needs, including application design, coding, testing, and deployment.
- **Business Intelligence:** Implementing tools and processes for data visualization, reporting, and analytics to support strategic business decisions.
- **Business Process Automation:** Streamlining and automating business processes to improve efficiency and reduce manual effort.

- **Robotic Process Automation:** Deploying software robots to perform repetitive and rule-based tasks, improving operational efficiency and accuracy.

4. Data Processing Activities

4.1 Nature of Data Processed

- **Personal Identifiable Information (PII):** Includes names, contact details, and other personal data necessary for service delivery.
- **Business and Operational Data:** Includes data related to client operations, projects, and interactions.
- **Analytical and Research Data:** Includes data used for generating insights, reports, and research findings.

4.2 Purpose of Data Processing

- **Data Services:** To develop and implement data strategies, engineer data solutions, analyze data for insights, apply scientific methods to data, and deploy machine learning models.
- **Software Services:** To develop and maintain software solutions, implement business intelligence tools, automate business processes, and deploy robotic process automation.

4.3 Data Retention Period

- **Client Data:** Retained for 5 years post-project or as per contractual agreements.
- **Operational Data:** Retained for 2 years or as required for operational purposes.
- **Analytical Data:** Retained for 3 years to support ongoing analysis and reporting needs.

5. Risk Assessment

5.1 Identification of Risks

- **Unauthorized Access:** Risk of unauthorized individuals accessing sensitive personal and business data.
- **Data Breaches:** Potential for data breaches leading to the exposure or loss of personal data.
- **Inadequate Protection Measures:** Risk that data protection measures in place may not be sufficient to safeguard data.
- **Regulatory Non-Compliance:** Risk of non-compliance with data protection regulations, leading to legal and financial repercussions.

5.2 Assessment of Risks

- **Likelihood of Occurrence:** Medium
- **Impact on Privacy:** Severe, due to potential exposure of sensitive information.

6. Mitigation Measures

6.1 Data Security Measures

- **Encryption:** Data encryption both in transit and at rest to protect against unauthorized access.
- **Access Controls:** Implementation of role-based access controls and strong authentication mechanisms.
- **Regular Audits:** Conduct regular security audits and vulnerability assessments to identify and address potential security weaknesses.

6.2 Compliance Measures

- **Regulatory Adherence:** Compliance with GDPR and other relevant data protection regulations.
- **Staff Training:** Regular training for staff on data protection practices and handling of personal data.
- **Data Subject Rights:** Processes in place to address data subject rights, including the right to access, rectify, and erase personal data.

7. Consultation with Stakeholders

7.1 Internal Consultation

- Engaged with IT, legal, and compliance departments to ensure comprehensive risk assessment and mitigation measures.

7.2 External Consultation

- Consultation with external data protection consultants as needed for expert advice on compliance and best practices.

8. Review and Approval

8.1 Review Process

- The DPIA will be reviewed annually and updated as necessary based on changes to data processing activities or regulatory requirements.

8.2 Approval

- Approved by the Data Protection Officer (DPO) or relevant authority within Be Data Solutions.

9. Documentation and Record-Keeping

- Detailed records of the DPIA process, including risk assessments, mitigation measures, and decisions, will be maintained.
- Any changes or updates to data processing activities will be documented accordingly.

10. Contact Information

For further inquiries or concerns regarding this DPIA, please contact:

- **Data Protection Officer (DPO):** MD RANA MAHMUD

- **Contact Email:** hello@bedatasolutions.com | info@bedatasolutions.com
- **Contact Phone:** UK: +44 (0) 207 754 0306 | BD +8809614502033