



POLICY DOCUMENT

Data Protection Impact Assessment Policy

1. Introduction

Albatross Bus & Coaches Ltd is committed to ensuring that personal data is processed in compliance with the **UK General Data Protection Regulation (UK GDPR)** and the **Data Protection Act 2018**. As part of this obligation, the organisation conducts Data Protection Impact Assessments (DPIAs) where processing activities are likely to result in a high risk to the rights and freedoms of individuals.

A DPIA is a structured process designed to identify, assess and mitigate privacy risks at an early stage of any project or operational change. It ensures that data protection principles such as data minimisation, purpose limitation and security are embedded into business processes by design and by default.

DPIAs are required when introducing new technologies, systems or processes, or where significant changes are made to existing operations involving personal data.

DPIAs will typically be triggered in the following circumstances:

- Introduction or significant change to systems, software, or databases
- Changes to policies, procedures or services
- New data sharing arrangements or third party involvement
- Processing involving new categories or increased volumes of personal data

2. Scope

This policy applies to all projects, systems and processes within Albatross Bus & Coaches Ltd that involve the processing of personal data. A DPIA must be conducted where there is a consistent internal trigger indicating potential risk, particularly where large volumes of personal data are processed, sensitive data is involved or where processing activities are complex or involve external parties.

Consideration will be given to the scale of processing, the nature of the data and whether the activity includes data sharing, profiling or the use of new technologies. DPIAs form part of the organisation's broader risk management, procurement and project management processes and must be completed prior to implementation of any high risk activity.

2.1 DPIA Process Flow

Albatross Bus & Coaches Ltd follows a structured approach to conducting DPIAs to ensure consistency and compliance. The process begins with determining whether a DPIA is required and continues through risk assessment, mitigation and ongoing review.

Key stages include:

- Determining whether a DPIA is required (using checklist)
- Conducting an initial privacy overview
- Completing the DPIA questionnaire
- Identifying and assessing privacy risks
- Recording risks within a Privacy Risk Log
- Identifying and implementing mitigation measures
- Monitoring and reviewing outcomes

2.2 Who leads the Project

A balanced and objective approach is essential when conducting a DPIA. Responsibility for leading the DPIA should be shared between the project lead, who understands the operational objectives, and the designated Data Protection Lead, who ensures that privacy risks are properly identified and addressed.

The Data Protection Lead will provide independent oversight to ensure that all privacy considerations are assessed objectively and that compliance requirements are fully met without compromising the successful delivery of the project.

2.3 Stakeholders that should be involved in the process

Appropriate stakeholders must be involved in the DPIA process to ensure that all relevant perspectives are considered. This may include representatives from operations, IT, compliance and management.

Where the risk is considered high, or where data sharing with external organisations is involved, external stakeholders such as clients or partners may also be consulted. Stakeholder involvement supports transparency, improves risk identification and enhances confidence in the organisation's approach to data protection.

DPIA Screening Checklist

Before conducting a full DPIA, an initial screening must be completed. Where **two or more** of the following conditions apply, a DPIA is required.

1. Different technologies are to be used for the first time by the organisation ..
2. Will there be any profiling conducted? Example – behaviours/web monitoring ..
3. The use of CCTV in a public place ..
4. Large scale of data processing. Either the volume of processing that is done or ..
a core activity
5. Will the organisation be processing sensitive data? ..
6. Will the organisation be transferring data outside the EEA? ..
7. Automated decision making, i.e. decisions made without human intervention? ..
8. Processing data concerning children, vulnerable adults, imbalanced power? ..
9. Data aggregation, linking databases, CRM systems porting data between systems ..
10. Processing that is unexpected or unavoidable or intrusive? ..
11. Will there be a collection of new categories of data? ..

12. Will the personal data be shared outside the organisations where not previously done? ..
13. Could the processing have a negative impact on the individual? ..

3. Privacy considerations for project initiation

3.1 Project Summary (What is the project and its context to the business)

Describe the project and what it intends to achieve by addressing the following points:

- Describe the project as a whole
- What are we trying to achieve by carrying out this project?
- Why was a DPIA decided upon – See DPIA checklist

3.2 Scope of the PIA

Describe what the DPIA does and doesn't cover. For example:

- What areas of the business, our systems, projects, IT infrastructure are included?
- What are the information management processes that the DPIA will cover (for example, will it cover storage, use, retention, disposal etc.)?
- Are there any limitations of the DPIA? For example, the DPIA may not cover third party use of personal information if third parties don't and won't access the information.

3.3 Describe the information flows

A clear understanding of how personal data flows through the organisation is essential. This includes how data is collected, used, stored, shared, and deleted, particularly where third parties are involved.

Key considerations include:

- How will the project change the flow of information?
- How will the information be collected and transferred to the organisation?
- Who will have access to the information from inside the business?
- Who will have access to the information from outside the business?
- Where will the information be held?

- What measures will be in place to ensure the information is accurate and up to date?
- What will the information be used for and how will this be communicate to the individuals?
- How long will the information be retained? How will it be destroyed/deleted?
- Who will be the owner of the information?
- Will the information be shared with anyone? If yes, who?

Insert an information flow diagram below (to show where information is coming from, where it is going to, how it is going to be used, who will use it. This will help with security and reducing privacy risks).

4. DPIA Questionnaire

A DPIA questionnaire must be completed to assess potential privacy risks associated with the project. This includes evaluating whether the processing involves new technologies, intrusive monitoring, data sharing, profiling, or automated decision making.

The questionnaire should also assess whether the processing exceeds individuals' reasonable expectations, involves vulnerable groups, or includes international data transfers. Responses should be clearly recorded as Yes / No / Not Applicable, with supporting comments where necessary.

Sr. No	Questions	Notes/Comment	Response
1.	Does the project require new technology and does is it intrusive on people's privacy?		Yes/No/NA
2.	Is the new process intrusive on privacy, require new identifiers, authentication or management process?		Yes/No/NA
3.	Will any new technology be privacy intrusive, such as body cams, tracking, locating software, monitoring software?		Yes/No/NA
4.	Will the project reduce or eliminate anonymity where it once existed or identify transactions previously anonymous or pseudonymised?		Yes/No/NA
5.	Are there other organisations involved in this project and will the data be transferred/shared with them if not already doing so?		Yes/No/NA
6.	Will there be new or change handling of personal data because of this project?		Yes/No/NA
7.	Does the project involve joining, cross referencing or linking personal data from multiple sources or		Yes/No/NA

	locations?		
8.	Are there any exemptions that can apply to the processing as a result of this project?		Yes/No/NA
9.	Do any of the following apply?		Yes/No/NA
	Is the data used for any profiling, including advertising behavioural analysis?		Yes/No/NA
	Are there any genetic, biometric data used?		Yes/No/NA
	Will the data be used to assess risk to the data subject?		Yes/No/NA
	If special category data is used, is it used for a purpose other than its initial intended purpose?		Yes/No/NA
	Is there a need to make personal data publicly available?		Yes/No/NA
	Will the project result in tracking of employees?		Yes/No/NA
10.	Any automated decisions made using personal data that will have a legal or similar affect?		
11.	Is there any tracking or monitoring taking place?		Yes/No/NA
12.	Is the data being used for scoring (economic position, health, performance at work, financial, interests)		Yes/No/NA
13.	Who will be affected by the project?		Yes/No/NA
14.	Will the project require joining of data sets (anonymised or otherwise) which could create a greater risk to the data subject?		Yes/No/NA
15.	Will this project lead to or require processing which is beyond a reasonable expectation of the data subjects?		Yes/No/NA
16.	Does the individual have a choice in providing their data?		Yes/No/NA
17.	Will personal data be transferred outside the EEA?		
18.	Will there be processing of personal data of children (under 16yrs old) or vulnerable adults?		

5. Additional Privacy Considerations

In addition to the core DPIA process, further privacy considerations must be addressed to ensure full compliance. This includes identifying a lawful basis for processing under UK GDPR and, where applicable, an additional condition for processing special category data.

Privacy notices must be reviewed and updated where necessary to ensure transparency. The organisation must also consider whether the same objective can be achieved with less personal data or reduced processing.

Key considerations include:

- Identify a legal basis for processing and if sensitive data an additional legal basis. Detail the basis and if necessary carry out a balancing test or determine if processing can continue if consent is relied upon.
- Update privacy notices if necessary - all formats
- Could the project be conducted without the need for the processing of all personal data collected?
- Can processing be limited?
- How will you ensure the accuracy of the data both during and after the project?
- Amend retention schedules and subject access process accordingly
- Provide sufficient training (and get it signed off) by those who will be involved
- Consider the data subjects rights and ensure that they can be easily exercised

6. Monitoring and Review

DPIAs are not a one time exercise and must be reviewed regularly throughout the lifecycle of a project. As projects evolve, risks may change and the DPIA must be updated accordingly. Ongoing monitoring ensures that mitigation measures remain effective and that the organisation continues to meet its

data protection obligations.

7. Document Ownership and Approval

This policy will be reviewed annually or in response to significant changes in legal, regulatory, or operational requirements. The Data Protection lead is responsible for maintaining and updating the document.

Approved by

Managing Director: _____

Signature: _____

Approval Date: 15 April 2026

