



AIB Group Data Protection Statement

The AIB Group places the utmost importance on the protection of the personal data of our customers and our staff. The Group Data Protection Policy ("Policy") that codifies this commitment is part of the Regulatory Compliance Risk Management Framework and defines our approach to the effective management of Data Protection.

The policy applies to the AIB Group, including all legal entities and subsidiaries, together referred to as the "Group". The policy applies to all processing of personal data within the group, irrespective of where it takes place.

The purpose of the Policy is to provide clear policy rules and principles that are to be applied to the protection of personal data within the Group. It is in line with the Data Protection Acts 1988-2018, the UK Data Protection Act 2018 and the General Data Protection Regulation ("the GDPR"), (EU) 2016/679. These outline the rules regarding the protection of fundamental rights and freedoms of natural persons, and in particular, reinforces the Data Protection rights of individuals and facilitates the free flow of personal data within the EU and adequate countries.

The policy incorporates rules aligned to the core GDPR principles, including:

- Data Security – the DPO reviews all potential personal data breaches and where such a breach could result in a very high risk to the rights and freedoms of a data subject, the DPO must ensure that they are made aware of this as soon as possible.
- Data Minimisation – Group staff must ensure that the personal data being used is adequate, relevant and limited to what is necessary. They must record details of this processing and the business requirements in the business areas' Records of Processing.

The requirements of the Group Data Protection Policy apply to all staff within the Group including contractors, consultants, agents or other third parties who have access to personal data either directly or indirectly, in the capacity of a Data Controller and/or Data Processor. All staff understand the responsibilities and obligations that must be adhered to under Data Protection Regulation. Where the scope of the policy is not adhered to, it constitutes a policy breach.

All staff are responsible for ensuring the Group meets the requirements of Data Protection Regulation while also ensuring that appropriate processes and procedures are in place to deliver compliance with those requirements on an ongoing basis. All staff in the Group are responsible for:

- Complying, at all times, with the policy and with the procedures that have been established by business units to comply with Data Protection Regulation;
- Completing annual Data Protection training;

- Fully understanding their personal responsibility for compliance with Data Protection Regulation within their area of responsibility, and the potential consequences of non-compliance with this policy.

The policy is aligned with the Group Risk Appetite Statement (RAS)

The Group Internal Audit (GIA) through the Board Audit Committee provide the Group Board of Directors with an independent view on the key risks facing AIB, including Data Protection risk, and the adequacy and effectiveness of governance, risk management and the internal control environment in managing these risks.

The Group Data Protection Office is the advocate for Data Protection risk awareness throughout the Group. They provide advice and guidance to business areas on Data Protection Regulation and the application of guidance from the Data Protection Commission.

Owner: Louise O'Brien
Group Data Protection Officer

Approver: Neil Donnelly
Group Chief Compliance Officer

Date : 30 June 2023