DATA PROTECTION POLICY

POL001

Title:	**POL001: Data Protection Policy**		
Created:	20 Jan 2021	**Reviewed:**	3 Feb 2022
Version:	1.0	**Pages:**	Page **1** of **7**

Data Protection Policy

Introduction

Akimbo Core Ltd ("Akimbo") is required to store and process personal information in order to conduct business. This includes personal data about employees, customers, and suppliers.

Akimbo is required to remain compliant with the General Data Protection Regulation and the Data Protection Act 2018.

Scope

This policy applies to all staff of Akimbo, including employees, contractors, temporary staff, volunteers, apprentices, and work experience (collectively "Staff"). It applies to all handling of personal data including the collection, processing, storage, and destruction. It applies to all formats including physical and digital formats.

Personal Data means any information relating to an identifiable living person (a "Data Subject") who can be identified, directly or indirectly, from that data. For example, a name, identification number, location data, or online identifier.

Failure to comply with this policy may result in disciplinary action, up to any including dismissal without notice for gross misconduct.

Responsibility

Responsibility for ensuring data protection compliance falls to the Directors. All staff covered by the scope of this policy have a duty to report any breach of this policy to a Director as soon as possible.

References

- General Data Protection Regulation 2016
- Data Protection Act 2018

Review

This policy is to be reviewed every year, or in-line with any changes in legislation.

Policy

GDPR outlines seven principles for data processing, specific legal bases for processing personal data, special categories of personal data, and specific rights for data subjects. These are outlined below along with the procedures and actions required to support them.

The Principles

1. Lawfulness, Fairness and Transparency – Akimbo will process personal data in a lawful fair and transparent manner.
2. Purpose Limitation – Akimbo will only process personal data for specific, explicit and legitimate purposes, which it will document.
3. Minimisation – Akimbo Core will only process data that is relevant and limited to what is necessary for the purposes for which they are processed.
4. Accuracy – Akimbo will ensure all data processed is accurate and up to date where possible.
5. Storage Limitation – Akimbo will not keep personal data for longer than it is necessary for the purposes for which it is processed.
6. Integrity and Confidentiality – Akimbo will process personal data in a secure manner, ensuring protection against unauthorised or unlawful processing, accidental loss, destruction or damage, using appropriate technical or organisational measures.
7. Accountability – Akimbo will be responsible for and demonstrate compliance with the above principles.

Processing Personal Data

Personal data must only be processed if one of the following legal bases can be met:

1. The Data Subject has given consent to the processing of their data, and that consent is demonstrable, in written form, and was requested in an intelligible and easily accessible form using clear and plain language – and that consent has not been withdrawn. Consent may be withdrawn at any time and must be as easy as giving content.
2. The processing necessary for a contract the Data Subject is party to, or in order to take steps prior to entering into a contract.
3. The processing is necessary for compliance with a legal obligation.
4. The processing is necessary to protect the vital interests of the data subject or another person.

Special Category Data

Special Category information is sensitive information and therefore requires special consideration; GDPR defines special category data as any of the following:

- Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, generic data, or biometric data; or
- Data concerning health, sex life, or sexual orientation.

Due to the sensitive nature of this information explicit consent should be sought where possible, in line with Basis (1) set out above. Before processing this data, a Data Protection Impact Assessment (DPIA) should be considered. Where processing is likely to be high risk a DPIA must be conducted.

Criminal Offence Data

GDPR gives extra protection to personal data relating to criminal convictions and offences or related security measures. This is referred to as “Criminal Offence Data”.

Processing of Criminal Offence Data may be required in relation to employment under the terms of the Rehabilitation of Offenders Act, in relation to specific roles within the organisation which meet the criteria set out by the Disclosure and Barring Service.

Before processing this data, a Data Protection Impact Assessment (DPIA) should be considered. Where processing is likely to be high risk a DPIA must be conducted.

Data Subjects Rights

GDPR gives Data Subjects the following rights in relation to their personal data:

1. The right to be informed about the processing of their personal data
2. The right to access a copy of their data (Subject Access Request)
3. The right to rectification if their data is incorrect
4. The right to erasure (also known as “The right to be forgotten”)
5. The right to the restriction of processing
6. The right to data portability – to transfer from one similar supplier or service provider to another.
7. The right to object to automated decision making

Training

All staff covered by the scope of this policy, whose roles may require the handling of personal data, require security training. This must be included within induction training to ensure that training is delivered before access to personal information is granted. Refresher training must be conducted at least annually.

Employee Responsibilities

All staff covered by the scope of this policy, must:

- only access personal data that they have authority to access and only for authorised purposes.
- not disclose personal data to anyone inside the organisation unless that person also has appropriate authority to process the data.
- not transfer personal data to anyone outside the organisation, unless a documented exception exists which has been authorised by a Director.
- not transfer personal data outside of the UK unless a documented exception exists which has been authorised by a Director.
- not transfer personal data to personal devices, or any device other than issued company equipment.
- not process Special Category Data or Criminal Offence Data unless they have documented authorisation from a Director.
- ensure that the security of personal data is protected.
- ensure that personal data is not unlawfully processed.
- ensure that personal data is not lost, or unlawfully or unintentionally altered.
- follow a clear desk policy of ensuring that desks are free of all printed media such as paper documents and removable computer media such as USB sticks and CDs at all times. Unless a document is actively being used it must be stored securely.

Data Breaches

If a breach of personal data is discovered it must be reported to the Information Commissioner's Office (ICO) without undue delay but not later than 72 hours after discovery, unless it is unlikely to result in a risk to individuals.

To enable this, personal data breaches must be reported to a Director as soon as possible. The Director will be responsible for ensuring that it is reported to the ICO if required. All data breaches must be recorded regardless of their impact.

Where a personal data breach is likely to result in a high risk to the rights and freedoms of affected individuals, the Director is responsible for ensuring those individuals are informed of the breach, without undue delay.

Document Control

Author	Date	Version	Status
Holly Grace Williams	20 Jan 2021	0.1	Draft
Holly Grace Williams	20 Jan 2021	1.0	Approved
Holly Grace Williams	11 July 2021	-	Reviewed
Holly Grace Williams	3 Feb 2022	-	Reviewed