Fincomp Services Limited
Data Protection Policy

Introduction

Fincomp Services Limited ("us" or "we") take our responsibilities with regard to the management of the requirements of the Data Protection Act 1998 ("the Act") very seriously. This document provides the policy framework through which effective management of Data Protection matters can be achieved.

1. Scope

The purpose of this policy is to ensure that all staff comply with the provisions of the Act when processing Personal Data. Any serious infringement of the Act will be treated seriously and may be considered under disciplinary procedures.

We are required to adhere to the eight principles of data protection as laid down by the Act. In accordance with those principles Personal Data shall be:

1. Processed fairly and lawfully
2. Processed for specified purposes only
3. Adequate, relevant and not excessive
4. Accurate and up to date
5. Not kept longer than necessary
6. Processed in accordance with data subjects' rights
7. Processed and held securely
8. Not transferred outside the countries of the European Economic Area (EEA) without adequate protection.

2. Responsibilities

2.1. Our responsibilities

As the Data Controller we are responsible for establishing policies and procedures in order to comply with the requirements of the Act.

2.2 Chief Information Officer (CIO) Responsibilities

The CIO holds responsibility for:

- Establishing policies and procedures in order to comply with the requirements of the Act;
- Data Protection notification - details of our notification are published here. Anyone who is, or intends on, processing Personal Data for purposes not included in the notification should seek advice from the CIO;
- Drawing up guidance, giving advice and promoting compliance with this policy in such a way as to ensure the easy, appropriate and timely retrieval of information;

- The appropriate compliance with subject access rights and ensuring that data is released in accordance with subject access legislation under the Act;
- Ensuring that any data protection breaches are resolved, catalogued and reported appropriately in a swift manner and in line with guidance from the Information Commissioner's Office;
- Investigating and responding to complaints regarding data protection including requests to cease processing Personal Data.

2.3 Staff Responsibilities

Staff members who process Personal Data about any individual must comply with the requirements of this policy.

Staff members must ensure that:

- All Personal Data is kept securely;
- No Personal Data is disclosed either verbally or in writing, accidentally or otherwise, to any unauthorised third-party;
- Personal Data is kept in accordance with our retention schedule;
- Any queries regarding data protection, including subject access requests and complaints, are promptly directed to the CIO;
- Any data protection breaches are swiftly brought to the attention of the CIO and that they support them in resolving breaches;
- Where there is uncertainty around a Data Protection matter, advice is sought from the CIO.

Staff who are unsure about who are the authorised third parties to whom they can legitimately disclose Personal Data should seek advice from the CIO.

2.4 Third-Party Data Processors

Where external companies are used to process Personal Data on our behalf, responsibility for the security and appropriate use of that data remains with us.

Where a third-party data processor is used:

- A data processor must be chosen which provides sufficient guarantees about its security measures to protect the processing of Personal Data;
- Reasonable steps must be taken that such security measures are in place;
- A written contract establishing what Personal Data will be processed and for what purpose must be set out;
- A data processing agreement, available from the CIO, must be signed by both parties.

For further guidance about the use of third-party data processors please contact the CIO.

3. Subject Access Requests

We are required to permit individuals to access their own Personal Data held by us via a Subject Access Request. Any individual wishing to exercise this right should do so in writing to the CIO. A standard form, along with our **Subject Access Request Policy** is available here or from the CIO.

We aim to comply with requests for access to personal information as quickly as possible but will ensure that it is provided within the 40 calendar day limit set out in the Act

Individuals will not be entitled to access information to which any of the exemptions in the Act applies. However, only those specific pieces of information to which the exemption applies will be withheld and determining the application of exemptions will be made by the CIO.

4. Data Protection breaches

Where a Data Protection breach occurs, or is suspected, it should be reported immediately in accordance with the **Data Breach Policy** which states:

Confirmed or suspected data security breaches should be reported promptly to the CIO at 020 8099 7301, email: cio@fincomp.co.uk. The report should include full and accurate details of the incident including who is reporting the incident and what classification of data is involved.

5. Contact

Queries regarding this policy or the Act at large should be directed to the CIO at 020 8099 7301, email: cio@fincomp.co.uk.