Data Protection Policy

Title	Data Protection Policy
Classification:	Internal Use Only
Author	Ashka Trivedi (Compliance Officer)
Reviewer (suitability and adequacy)	Laduram Vishnoi (CEO)
Approver (suitability and adequacy)	Laduram Vishnoi (CEO) 
Policy/Document Owner	Ashka Trivedi (Compliance Officer)
Current Version	1.1
First Document Release Date	25/05/2018
Revised Date	25/05/2019
Next Revision Date	25/05/2020

Modification History:

S. No.	Description of Change	Date of Change	Version No.
1	Annual Review- No changes applied	25/05/2019	1.0
2			
3			

Table of Contents

1. Introduction

Acquire needs to gather and use certain information about the individual and is committed to protecting the rights and freedom of data subjects.

We hold personal data about our employees, clients, suppliers and other individuals for variety of business purposes.

This policy describes how safely and securely we collect, handle and store personal data in accordance to meet the legal obligation's covered under data protection standards. These policies also sets out the rules for our staff on their use and access of personal data during their course of work and make them aware that before implementing any significant changes to data and its processing they need to consult Data Protection Officer (DPO) to ensure relevant measures of compliance.

1.1.Purpose

The purpose for this data protection policy is to ensure:

- Compliance with data protection law and follow good practice
- Protection of the rights of staff, customers and partners
- Openness on how it stores and process individuals' data
- Protection against the risks of data breach

1.2.Scope

This policy applies to all staff, contractors, suppliers who must be familiar with this policy and comply with its terms. It also applies to all data that the company holds relating to identifiable individuals such as Name, email addresses, postal addresses, Telephone numbers, or any other information relating to individual. This policy helps to protect Acquire from data security risks such as Confidentiality Breach, Failing to offer choice, and reputational damage.

1.3.Responsibilities

Acquire is the Data Controller under the Act, which means that it determines what puposes personal information held, will be used for. It is also responsible for notifying the Information Commissioner Office (ICO) of the data it holds or is likely to hold, and the general purposes that this data will be used for

Everyone who works for or with Acquire has some responsibility for ensuring data is collected, stored and handled appropriately.

However, these people have key areas of responsibility:

- The **Chief Executive Officer** is ultimately responsible for ensuring that Acquire meets its legal obligations.
- The **Data Protection Officer[Ashka Trivedi]** is responsible for

  - Keeping the board updated about data protection responsibilities, risks, and issues.
  - Reviewing all data protection procedure and related policies
  - Arranging data protection training and advice for the people covered by this policy.
  - Responding to the requests from individuals to see the data Acquire holds about them.
  - Answering questions on data protection from staff, board member and other stakeholders.
  - Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.
- The **IT Manager,** is responsible for:
  - Ensure all systems, services, and equipment used for storing data meet acceptable security standards.
  - Performing regular checks and scans to ensure security hardware and software is functioning properly.
  - Evaluating any third-party services, such as cloud services the company is considering using to sore or process data.
- The **[Marketing Manager][Sam Suthar]** is responsible for:
  - Approving data protection statements attached to emails and other marketing copy.
  - Addressing data protection queries from clients, target audiences or media outlets
  - Coordinating with DPO to ensure all marketing initiatives adhere to data protection laws and the company's Data Protection Policy.

2. The GDPR Principles

Acquire shall comply with the principles of data protection (the principles) enumerated in the EU General Data Protection Regulation. Our best effort is to protect personal data in accordance with these principles and comply with the Data Protection Standards. The Principles are

1. **Lawful, fair and transparent**
   There must be transparent, lawful and fair process for Personal data collection and its use.

2. **Limited for its purpose**
   Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

3. **Data Minimization**
   Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

4. **Accurate**
   Any data we hold must be accurate and kept up to date.

5. **Retention**
   Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

6. **Secure**
   Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures.

3. Definitions

Data
In terms of Act data are information relating to an individual where the structure of the data allows information about the individual to be readily processed.

Personal Data
Any data relating to an identified or identifiable natural person ('Data Subject') such as name, address, email address, phone number, educational background, financial details, educational details, nationality etc.

Sensitive Personal Data
A subset of personal data that relate to a living person, recording such things as racial or ethnic origin, political opinions, religious beliefs, trade union membership, health, criminal convictions, etc.

Data Controller
'Data controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by law.

Data Processor
'Data Processor' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by law.

Data Processing
'Processing' means any operation or set of operations which is performed on personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaption or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Data Subject
The data subject is the individual whom particular personal data is about.

Supervisory Authority
This is the national body responsible for data protection. The supervisory authority for our organization is the Information Commissioners Office.

4. Policy and Procedures

4.1.General Guidelines

a) Data covered by this policy shall only be accessible to people who has a requirement for their tasks.
b) Access to confidential data should be formally shared on request to the employees.
c) Employees shall be provided with relevant awareness training on handling data and understand their responsibilities.
d) Detailed guidelines for keeping data secure and taking sensible precautions are provided in Access Control Policy.
e) Acquire take appropriate measures for fair collection and use of information
f) The purpose and the intent for which information is collected and used is specified to meet its legal obligations
g) Acquire collects and process data only to the extent that is needed to fulfill its operational needs.
h) Ensuring the accuracy and quality of the information used.
i) Ensuring the rights of people about whom information is held, is specified in privacy notices as per the regulations.
j) Implementing appropriate technical and organizational security measures to safeguard personal information.

4.2.Data Collection

To comply with data protection laws and accountability and transparency of data according to the principles of GDPR, we must demonstrate compliance.

Acquire ensures that the data collected is under the Informed consent and within the perimeter defined in this policy. It is applicable to data that is collected in person, or by registering our services. When collecting data, Acquire will ensure that the Individual/service User:

a. Clearly understands why the information is collected.
b. Individual/Service user understands the consequences and intent of its use and accordingly decides not to give consent to processing.
c. As far as reasonably possible, grants explicit consent, either written or verbal for data to be processed
d. Is, as far as reasonably practicable, competent enough to give consent and has given so freely without any coercion.
e. Has received sufficient information on why their data is needed and how it will be used.

4.3.Data Storage

Acquire ensures that the data and records collected from individual are stored appropriately in line with data protection laws. Below are the guidelines for data storage by Acquire:

a. Information and records relating to service users will be stored securely and will only be accessible to authorized staff and volunteers.
b. Data stored on paper should be kept at secure place and not left unattended where unauthorized people could access them.
c. Data will be stored for only as long as it is needed or statutory requirement and will be disposed of appropriately.
d. Data shall only be stored on designated drives and servers, and should be uploaded to an approved cloud computing services.
e. Acquire ensures that all personal and company data is protected by approved security software and firewall and is non-recoverable from any computer system previously used within the organization, which has been passed on/sold to a third party.

4.4.Data Use

When dealing with personal data, Acquire ensures that it is accessed and used as per the requirement by the organization and in accordance with data protection laws.

a. Personal data should not be informally shared or transferred via email in plain text.
b. Personal data must be always transferred in encrypted form and shall not be sent to external contacts without authorization.
c. Employees should not save any copies of personal data to their own systems.
d. Acquire will ensure that it has a Data Protection Officer with specific responsibility for ensuring compliance with Data Protection.
e. Personal data shall never be transferred abroad or anywhere else outside without express permission from the DPO.

4.5.Data Accuracy

Acquire will take reasonable steps to ensure data is kept accurate and up to date as per law requirement.

a. Data shall be held at as few places as necessary.
b. Ensuring that personal data is updated, accurate, relevant, and adequate. For instance, by confirming a customer's details when they call.
c. Acquire will make it easy for data subjects to update the information they hold for them. For instance, via company website.
d. It is marketing manager's responsibility to ensure marketing databases are checked against industry suppression files regularly.
e. Acquire implements measures to ensure privacy by data minimization and pseudonymisation.

4.6.Subject access requests

An individual has the right to receive confirmation that their data is being processed, access to their personal data and supplementary information which means the information which is provided in a privacy notice. As per the law requirement subject access requests shall be dealt as follows:

a. Subject access requests from individuals should be made by email, addressed to data controller at **ashka@acquire.io**
b. Acquire must provide an individual with a copy of information the request, free of charge, within a one month of receipt.
c. The data controller will always verify the identity of anyone making a subject access request before handling over any information.

4.7.Disclosure of Data

In certain circumstances, the GDPR allows personal data to be disclosed to law enforcement agencies without the consent of data subject.

Under these circumstances, Acquire will disclose requested data. However, it will ensure the request is legitimate, seeking assistance from the board and from the company's legal advisers where necessary.

4.8.Third Parties

As a **Data Controller**, we have written contracts in place with any third party **Data Processor** that we use. The contract contains specific clauses which set out our and their liabilities, obligations and responsibilities.

As a Data Controller, we must only appoint processor who can provide sufficient guarantees under GDPR and that the rights of data subjects will be respected and protected.

5. REFERENCES

This policy document is drafted in reference to GDPR Principles and their adoption in the organization.