Data subject Access Request Policy and Procedure

Title	Data Subject Access Request Policy and Procedure
Classification:	Internal Use Only
Author	Ashka Trivedi (Compliance Officer)
Reviewer (suitability and adequacy)	Security Officer
Approver (suitability and adequacy)	Chief Executive Officer
Policy/Document Owner	Security Officer
Current Version	1.0
First Document Release Date	25/05/2018

Modification History:

S. No.	Description of Change	Date of Change	Version No.
1			
2			
3			

Table of Contents

1. Introduction

The GDPR (General Data Protection Regulation) creates some new Rights for Data Subjects as well as strengthening existing Rights. As a Data Processor, the Tagove must be able to comply with these rights.

1.1. Purpose

This policy and procedure applies establishes as effective, accountable and transparent framework for ensuring compliance with the requirement for Tagove by GDPR.

1.2. Scope

This policy and procedure applies across all entities or subsidiaries owned, controlled, or operated by Tagove and all employees, including temporary, permanent or contract employees that handle Tagove data.

2. Policy

a) For all data subjects the GDPR details rights of access to both manual and electronic data. This is also known as Data Subject Access Request.
b) For GDPR compliance, organizations are required to respond to subject access requests within one month. Fail to do so can be a breach of GDPR and could lead to a complaint being made to Data Protection Regulator.
c) This policy informs staff of the process for supplying individuals with rights of access to personal data and the right of access to staff information under GDPR. Specifically:
d) All staff needs to be aware of their responsibilities to provide information when a data subject access request is received. When a subject access request is received, it should immediately be reported to data protection officer to log and track each request.
e) Request must be made in writing.
f) The statutory response time is one month.
g) Request must include the full name, date of birth and address of the person seeking access to their information. To comply with GDPR, information relating to the individual must only be disclosed to them or someone with their written consent to receive it.
h) No fee can be charged for initial data subject access request for all types of record, whether manual or electronic format.

3. Procedure

a. When a subject access request is received by staff or volunteers covering any of the Data Subject Rights given below, the request must be immediately be reported to the Tagoves' Data Protection Team. The GDPR provides following Rights for Individuals:
    - Right to be informed
    - Right of Access
    - Right to Rectification

- Right to Erasure (forgotten)
- Right to Restrict Processing
- Right to Data Portability
- Right to object
- Rights in Relation to Automatic Decision Making and Profiling

b. The request must be forwarded to ashka@acquire.io. If the request was made over the phone then as much information as possible regarding what was requested must be typed into email and sent to Data Protection Team Immediately. If the request is received in the postal letter, this can either be scanned or sent to the Data Protection Team by email.
c. The Data Protection Team will process the request accordingly and respond to the Data Subject in line with the legislation. They may ask for input and/or provision of data from teams across the Tagove in order to ensure they have fully complied with the request. Due to the time limits for complying, teams requested to assist should treat such requests as a priority.
d. If there is uncertainty around whether it is a request please refer to Data Protection Team for advice.
e. Before processing a request, the requestor's identity must be verified with suitable valid Identity Proof along with other proof of address.

4. Associated documents and policies

This policy is to be read in conjunction with the related policies;

- Data Protection Policy
- GDPR Policy & Procedure

5. Definitions

Data Subject: An individual who is the subject of personal data and whom particular personal data is about.

Personal Data: 'Personal data' means any information relating to an identified or identifiable person ('data subject'). An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person;

GDPR: General Data Protection Regulation is a regulation by the European Parliament intended to strengthen and unify data protection for individuals.

Processing: Obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including – a. organization, adaptation or alteration of the information or data, b. retrieval, consultation or use of the information or data, c. disclosure of the information or data by transmission, dissemination or otherwise making available, or d. alignment, combination, blocking, erasure or destruction of the information or data.

Legal Basis for Processing: Processing will only be lawful if at least one of the following applies:

a. the data subject has given consent to the processing of their personal data for one or more specific purposes
b. processing is necessary for the performance of a contract with the data subject or in order to take steps to enter a contract
c. processing is necessary to comply with a legal obligation
d. processing is necessary to protect the vital interests of the data subject
e. processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller
f. processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the of the data subject

Appendix 1 – Rights of Data Subjects:

Right of Access (Also known as a Subject Access Request)
Data Subjects have the Right to obtain:

- Confirmation that their data is being processed
- Access to their personal data and
- Other supplementary information

Right of access requests must be responded to within one month.

Right to Rectification
Data Subjects are entitled to have their personal data rectified if it is inaccurate or incomplete. If the information in question has been disclosed to a third party the Data Controller must inform them of the request for rectification where possible. The Data Subject is also entitled to be informed of the third parties to whom the data has been disclosed, where appropriate.

Rights to rectification must be responded to within one month.

Right to Erasure
This Right is also known as the 'Right to be Forgotten'. It enables Data Subjects to request the deletion or removal of personal data where there is no compelling reason for its continued processing by the Data Controller.
The Right to Erasure applies in the following circumstances:

- The personal data is no longer necessary in relation to the purpose for which it was originally collected
- The processing was based on consent, and the Data Subject has now withdrawn their consent
- The Data Subject objects to processing and there is no overriding legitimate interest of the Data Controller
- The data was being unlawfully processed
- The data must be erased to comply with a legal obligation

Right to Restrict Processing
When this Right is exercised you are permitted to store the personal data but not further process it. Restricted information about the individual may be retained to ensure that the restriction is respected in the future.
The Right to Restrict Processing applies in the following circumstances:

- When a Data Subject contests the accuracy of their personal data, then processing should be restricted to storage only until accuracy is verified
- When a Data Subject objects to processing which is being carried out for the reason of performance of a task in the public interest, or for the legitimate interests of the Data Controller, then the Data Controller must restrict processing to storage only whilst they consider whether their legitimate grounds override the Rights and freedoms of the individual.
- When processing is unlawful and a Data Subject opposes erasure and requests restriction to storage instead.

- When the Data Controller no longer needs the personal data but the Data Subject requires it for the purpose of a legal claim.

Right to Data Portability

This Right allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows the individual to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way in a common data format, for example, Excel or CSV file.

The Right to Data Portability applies in the following circumstances:

- When the personal data was provided to the controller directly by the Data Subject
- Where the processing is based on consent or performance of a contract
- When processing is carried out by automated means

Right to Object

Individuals have the Right to object to:

- Processing based on legitimate interest or performance of a task in the public interest/exercise of official authority (including profiling)
- Direct marketing (including profiling)
- Processing for the purposes of scientific/historical research and statistics

Rights in Relation to Automatic Decision Making and Profiling

This Right provides safeguards for individuals against the risk that a potentially damaging decision is taken without human intervention.

The Right not to be subject to a decision applies when:

- It is based on automated processing
- It produces legal/significant effects on the individual

It does not apply if the decision:

- Is necessary for entering into or performance of a contract
- Is authorized by law
- Is based on explicit consent
- Does not have a legal/significant effect on the data subject