Calvay Housing Association Limited

DATA SUBJECT RIGHTS

AND SUBJECT ACCESS REQUESTS POLICY

Approved: 18 June 2020

Review Date: June 2021

INTRODUCTION

The GDPR provides the data subject with more protection in relation to their personal data. That, in turn, gives greater obligations to us, as the data controllers (and processors) to comply with the requests of data subjects so that they can remain in control and so that processing is transparent.

These rights are set out in Chapter III: Articles 12 to 23 of the GDPR. Recitals 58 to 73 provide some additional guidance. The data subject rights under the GDPR are as follows:

the right to access personal data;
the right to rectification;
the right to erasure (right to be forgotten);
the right to restriction of processing;
the right to data portability;
the right to object to processing, including direct marketing; and
the right to object to automated decision making;

A sound understanding of this Policy is essential as its infringements can lead to an administrative fine of up to €20,000,000, or in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher.

The SAR Procedure Graph in Appendix 1 will be used in conjunction with the rest of this policy only.

REGULATION & BEST PRACTICE

This Policy has been developed taking account of relevant law and sector best practice.

The Regulation considered when drafting this Policy was the General Data Protection Regulation 2016/679, effective as of 25 May 2018

AIMS & OBJECTIVES OF THIS POLICY

This Policy aims to detail Calvay Housing Association's approach to Data Subject Rights. It is important that our Committee, Management and staff know when and how to process such requests, and exactly what our reciprocal rights and responsibilities are. This Policy should be implemented against the background knowledge of our general obligation of ensuring transparency with regards to the processing of any personal data we undertake.

WHAT IS A SUBJECT ACCESS REQUEST?

A Subject Access Request is a request from an individual, that seeks to ascertain what personal data we hold about them, why we hold it and who we disclose it to. Requests can be made either verbally or in writing.

For information to be personal data, it must *relate to* a living individual and allow that individual to be *identified* from it (either on its own or along with other information likely to come into the organisation's possession).

An individual is entitled to be provided with the following:

Whether any personal data is being processed;

A description of the personal data, the reasons it is being processed, and whether it will be given to any other organisations or people;

A copy of the personal data; *and*

Details of the source of the data (where this is available).

An individual can also request information about the reasoning behind any automated decisions taken about him or her, such as a computer-generated decision to grant or deny credit, or an assessment of performance at work (except where this information is a trade secret).

Remember - Subject Access Requests provides a right for the requester to see their own personal data, NOT a right to see copies of documents that contain their personal data. Often, the easiest way to provide the relevant information is to supply copies of original documents, but we are not obliged to do this.
Subject Access Requests can be made verbally or in writing. It is recommended that the response provided will be in a written form.

SUBJECT ACCESS REQUEST COMPLIANCE
Any communication with a data subject should be in a concise, transparent, intelligible and easily accessible form, using clear and plain language, particularly if addressed to a child. Therefore, any response to a request from a data subject will be easy to understand by everyone, but at the same time genuinely informative, providing all the information required.

There will generally be no fee charged to the requester/data subject. This is subject to the request being manifestly unfounded or excessive, particularly due to their repetitive nature.
If we are satisfied that the request is manifestly unfounded or excessive, a reasonable fee which covers administrative costs but not the costs of implementing a system, may be charged. In other cases, we can refuse to act upon the request completely.
This will only be done if we can reasonably demonstrate that the request falls into this category.
In such cases, the requester/data subject will be told why the we are refusing to act and be advised of their right to complain to the ICO and to seek a judicial remedy at the same time.

THE RIGHT TO RECTIFICATION (ARTICLE 16)
This refers to the individual's right to have inaccurate data, controlled or processed by us, rectified.
If we receive a request to have any personal data controlled or processed by us rectified, we will verify the accuracy of the data held.
If we are satisfied that the data needs to be rectified, WE will do so without delay.
If we cannot determine the accuracy of the data; or cannot timeously update the data, we will treat the data as 'in dispute'.
The processing of any 'in dispute' data will, upon data subject request, be restricted.
Once the data is rectified, we will inform all relevant third parties with whom we shared this data, of the rectification taking place. This will not be done if it is disproportionate or impossible to carry out.

DATA PORTABILITY (ARTICLE 20)
This only applies to data processed by automated means on a basis of a contract or consent.

If requested, we will provide any data processed by automated means in a structured, commonly used and digitally readable form, so that it may be transferred to another data controller without hindrance.

This data will also include information gathered by us in the course of any dealings with the individual or generated from monitoring of their activity. This does not include user profile created by analysis of the raw smart metering data collected, also known as inferred or derived data.

That right will not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

THE RIGHT TO ERASURE (ARTICLE 17)
This only applies to data:

a) Where it is no longer necessary to process on the basis of the purpose for which it was collected;
b) where consent has been withdrawn;
c) where there has been an objection to processing;
d) where there is no legal basis;
e) where there is a legal obligation to delete the data; *or* the information has been provided in relation to social media.

If a request for erasure, submitted by a data subject, satisfies one of the above circumstances, the relevant data will be deleted without undue delay (subject to the next section that follows).
If we have made the data public then we will also take reasonable steps to ensure that other controllers, who may have linked to, copied or replicated the data, also erase the data regardless of whether this has been specifically requested by the data subject.

This does not apply to personal data where processing is necessary for:

a) exercising the rights of freedom of expression;
b) to comply with a legal obligation in the public interest or in the exercise of an official authority;
c) for performance of a public interest task or exercise of official authority;
d) for public health reasons;
e) for archiving purposes;
f) for the establishment, exercise or defence of legal claims.

In such circumstances, the data will not be erased, and the requester will be duly informed of this, without delay, unless this is impossible or requires disproportionate effort.
Once the data has been deleted, we will also tell any recipient of the personal data that it has been erased, unless this is impossible or requires disproportionate effort. The data subject will be informed about those recipients if requested.

THE RIGHT TO RESTRICT DATA PROCESSING (ARTICLE 18)
This applies to data where:

a) The accuracy is in dispute;
b) The processing is unlawful;
c) The controller no longer needs the data, but it is required for legal rights; *and*
d) The processing has been objected to.

Once the relevant subject requests that we restrict data processing, based on one of the above grounds, we will limit our processing to the following:
For storage (with the consent of the data subject);
For the establishment of legal claims (or in certain restricted circumstances when it is in the public interest); *and* For the protection for the rights of another subject or legal entity.
Once the processing has been restricted, we will inform the data subject of the limitation being in place. That is, unless it is impossible or requires disproportionate effort to do so. In that event, we will inform the data subject once requested.
Once restriction is no longer qualified, or is withdrawn, we will inform the data subject of the restriction being lifted.

THE RIGHT TO OBJECT TO PROCESSING (ARTICLE 21)
Objecting to processing of data is available when it is processed for the following reasons:

a) In the public interest or in the exercise of official authority; or
b) It is carried out in reliance on the legitimate interests processing condition.

Once we receive a request from the data subject which meets the above criteria, we will cease the processing this data, unless we can demonstrate compelling legitimate grounds to continue with the processing, which override the interests, rights and freedoms of the data subject.
If the request to object to processing is related to direct marketing, we shall comply with this, ceasing all processing. However, we will keep a portion of the personal data only so far to ensure that the individual does not receive marketing messages in the future.
The data subject will be informed of all decisions made on the objections requested.

TIMESCALES FOR RESPONDING
The response will be made without undue delay. The relevant time limit for providing the relevant information is 1 month. (Recital 59). In rare circumstances this can be extended on one occasion by two more months (60 days) depending on the complexity of the request or the number of requests. In such cases, the requester/data subject will be told why we are delaying the request and be advised of their right to complain to the ICO and to seek a judicial remedy at the same time.

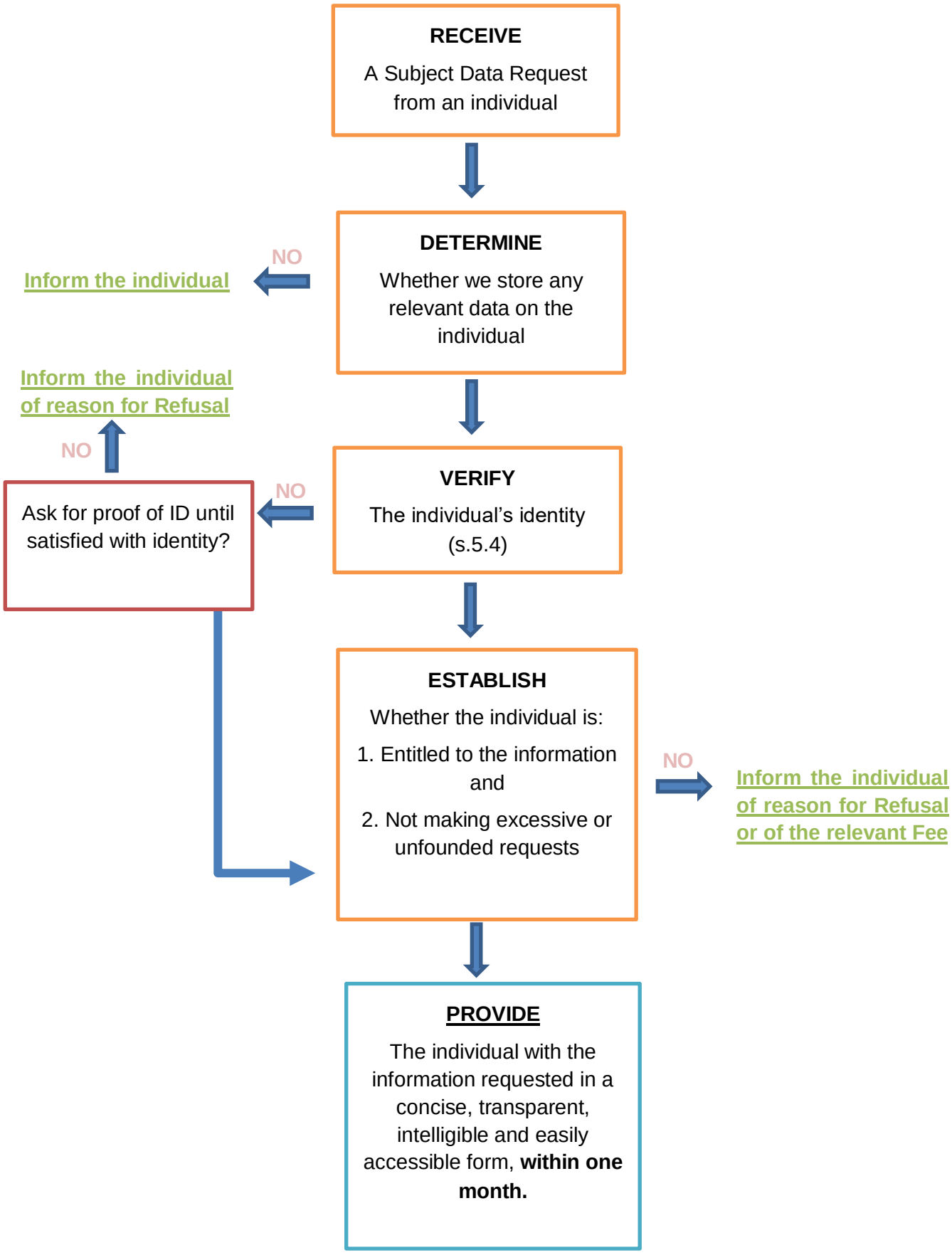
IDENTIFICATION
We will always confirm the identity of the person making the request prior to replying to the request.
If we have any reasonable doubt about the identity of the requester/data subject, we will ask for a copy of a passport or other photographic ID.
In instances where we are not satisfied with the proof provided by the subject, then we may refuse to disclose any related data until such satisfactory proof is provided.
In such circumstances we will inform the requester/data subject as to why we are refusing their request and be advised of their right to complain to the ICO and to seek a judicial remedy at the same time.
Such refusals will only be undertaken once we can reasonably prove the information provided was not of sufficient quality to reasonably grant the request, as the burden on proof rests on us, not the data subject.

WHAT TO DO IF YOU WISH TO COMPLAIN ABOUT OUR APPROACH TO SUBJECT ACCESS REQUESTS?
If any party involved wishes to complain about our approach to Subject Access Requests, they should refer to our Data Protection Co-ordinator who is responsible for overseeing this Policy and, as applicable, developing related policies and guidelines. That post is held by: Tracy Boyle, Corporate Services Manager, Tel: 0141 771 7722 or email: dpo@calvay.org.uk.

EQUAL OPPORTUNITES
We are committed to ensuring equal opportunities and fair treatment for all people in its work.
In implementing this policy, our commitment to equal opportunities and fairness will apply irrespective of factors such as gender or marital status, race, religion, colour, disability, age, sexual orientation, language or social origin, or other personal attributes.

REVIEW CYCLE

This Policy document will be reviewed annually or as required. Last updated October 2019.


RECEIVE
A Subject Data Request from an individual
DETERMINE
Whether we store any relevant data on the individual
NO
Inform the individual
VERIFY
The individual's identity (s.5.4)
NO
Ask for proof of ID until satisfied with identity?
NO
Inform the individual of reason for Refusal
ESTABLISH
Whether the individual is:
1. Entitled to the information and
2. Not making excessive or unfounded requests
NO
Inform the individual of reason for Refusal or of the relevant Fee
PROVIDE
The individual with the information requested in a concise, transparent, intelligible and easily accessible form, within one month.