

GDPR Data Processor Appointment Terms

Schedule 1

The terms and conditions that apply to this mortgage submission are set out in your Mortgage Intermediary Agreement together with the terms set out below in the GDPR Data Processor Terms (Schedule 1).

1. DEFINITIONS

In this **Schedule 1**, the following words and expressions will have the following meanings:

“Adequate Jurisdiction”	means a jurisdiction outside the European Economic Area that has been determined to have in place adequate protections for personal data including under the Data Protection Laws, pursuant to a valid decision notice issued by the European Commission.
“Agreement”	means the agreement for the Services that has been entered into by Dudley Building Society (“Customer”) and the Intermediary (“Supplier”) including the schedules and documents attached to or referred to in the same.
“Agreement Personal Data”	means the Personal Data (as defined under Data Protection Laws) being Processed from time to time pursuant to the terms of this Agreement, including as is more particularly described in the Annex to this Schedule 1 .
“Authorised Sub-Processor”	any third party appointed by the Supplier in accordance with this Agreement, with the prior written consent of the Customer, to Process Agreement Personal Data.
“Customer Group”	means each member of the Customer’s Group from time to time.

continued over

“Data Protection Laws”

all applicable laws (including decisions) and guidance by relevant supervisory authorities together with Applicable Laws relating to data protection, the processing of personal data and privacy, including:

- (a) the Data Protection Act 1998;
- (b) (with effect from 25 May 2018) the General Data Protection Regulation (EU) 2016/679;
- (c) the Privacy and Electronic Communications (EC Directive) Regulations 2003 (as may be amended by the proposed Regulation on Privacy and Electronic Communications); and
- (d) any legislation that, in respect of the United Kingdom, replaces or converts into domestic law the General Data Protection Regulation (EU) 2016/679, the proposed Regulation on Privacy and Electronic Communications or any other law relating to data protection, the processing of personal data and privacy as a consequence of the United Kingdom leaving the European Union;

and references to **“Data Controller”**, **“Data Subject”**, **“Personal Data”**, **“Process”**, **“Processed”**, **“Processing”** and **“Data Processor”** have the meanings set out in, and will be interpreted in accordance with:

- (i) in respect of processing undertaken on or before 24 May 2018, the Data Protection Act 1998;
- (ii) in respect of processing undertaken on or after 25 May 2018, the General Data Protection Regulation (EU) 2016/679; and
- (iii) in respect of processing undertaken on or after the date on which legislation comes into force that, in respect of the United Kingdom, replaces or converts into domestic law the General Data Protection Regulation (EU) 2016/679, that legislation.

“Data Security Incident”

a breach of security leading to the accidental or unlawful destruction, loss, temporary or permanent loss of availability, alteration, unauthorised disclosure of, or access to, Agreement Personal Data transmitted, stored or otherwise Processed.

“Group”

together a person and any other person that controls, is controlled by or is under common control with the first person from time to time.

“Standard Contractual Clauses”

means the EU standard contractual clauses for data processors established in third countries pursuant to European Commission Decision (2010/87/EU) of 5 February 2010 under the EU Directive (95/46/EC), or such other European Commission decision under the Data Protection Laws as may replace that European Commission Decision from time to time, in each case in unamended form.

“Supervisory Authority”

means the Information Commissioner’s Office or such other supervisory authority as may be responsible for enforcing compliance with the Data Protection Laws from time to time.

2. DATA PROTECTION

2.1 Compliance with laws and confidentiality

- 2.1.1 In performing the Services and its other obligations under this Agreement the Supplier will and will procure that any Authorised Sub-Processor will comply with the Data Protection Laws.
- 2.1.2 The Supplier will and will procure that any Authorised Sub-Processor will keep the Agreement Personal Data secret and confidential in accordance with the terms of this Agreement.

2.2 Authority and roles

- 2.2.1 Without prejudice to **clause 2.4.1.1**, the Customer authorises the Supplier, on its own behalf and on behalf of the other members of the Customer Group, to Process the Agreement Personal Data during the term of this Agreement as a Data Processor and solely for the purpose of providing the Services.
- 2.2.2 The Parties acknowledge and agree that the Customer and each of the other members of the Customer Group (as relevant) is/are the Data Controller(s) of the Agreement Personal Data.

2.3 Sub-Processing

- 2.3.1 The Supplier will not engage or use any third party for the Processing of Agreement Personal Data or otherwise cause or permit any third party to Process Agreement Personal Data without the prior written consent of the Customer.
- 2.3.2 If the Supplier appoints an Authorised Sub-Processor pursuant to **clause 2.3.1** the Supplier will ensure that there is in place a written contract between the Supplier and the Authorised Sub-Processor that specifies the Authorised Sub-Processor’s Processing activities and imposes on the Authorised Sub-Processor the same terms as are imposed on the Supplier in this **clause 2**.
- 2.3.3 The Supplier will remain responsible and fully liable to the Customer and the members of the Customer Group for all acts and omissions of Authorised Sub-Processors as if they were its own.

2.4 Supplier's obligations as Data Processor

- 2.4.1 The Supplier will, and will procure that any Authorised Sub-Processor will:
- 2.4.1.1 Process the Agreement Personal Data only on documented instructions from the Customer on its own behalf and on behalf of the relevant member(s) of the Customer Group who is/ are the Data Controllers (including for the avoidance of doubt the instructions as are set out in this Agreement;
 - 2.4.1.2 Immediately inform the Customer in writing if, in its reasonable opinion, any instruction received in connection with this **clause 2** infringes any Data Protection Laws;
 - 2.4.1.3 Without prejudice to **clause 2.4.1.1**, ensure that Agreement Personal Data will be used solely for the purpose of providing, and to the extent required to provide, the Services;
 - 2.4.1.4 Not cause or permit any Processing of Agreement Personal Data to occur outside the United Kingdom and/or the European Economic Area (as it is made up from time to time), including by way of any transfer, without the Customer's prior written consent;
 - 2.4.1.5 (In the event that the consent more particularly referred to in **clause 2.4.1.4** is given, the Supplier will, prior to causing or permitting any such Processing to occur outside the United Kingdom and/or the European Economic Area:
 - (a) verify that the transfer is to a recipient located within an Adequate Jurisdiction (subject to any applicable restrictions);
 - (b) ensure that the Standard Contractual Clauses are entered into as between the Customer (and/or the relevant member of the Customer Group) as 'data exporter' and the recipient of the Agreement Personal Data (including the Approved Sub-Processor, as relevant) as 'data importer' and that they remain in place throughout the term of the Agreement;
 - (c) provide evidence in writing to the Customer that the recipient of the Agreement Personal Data (including the Approved Sub-Processor, as relevant) is certified under the EU/US Privacy Shield framework and that the certification is valid in respect of Processing of Agreement Personal Data under this Agreement (and the Supplier hereby warrants and undertakes to ensure that the Standard Contractual Clauses are entered into in the manner more particularly described at **clause 2.4.1.5(b)** immediately in the event that the recipient of the Agreement Personal Data is no longer certified under the EU/US Privacy Shield framework); or
 - (d) provide evidence in writing to the Customer that the recipient of the Agreement Personal Data (including the Approved Sub-Processor, as relevant) has entered into Binding Corporate Rules which are valid in respect of Processing of Agreement Personal Data under this Agreement and which have been approved by the European Commission and/or appropriate regulators (and the Supplier hereby warrants and undertakes to ensure that the Standard Contractual Clauses are entered into in the manner more particularly described at **clause 2.4.1.5(b)** immediately in the event that the recipient of the Agreement Personal Data is no longer a party bound by the Binding Corporate Rules);)
 - 2.4.1.6 Should any of the transfer mechanisms more particularly referred to in **clause 2.4.1.5** which are being used by the Supplier for the purposes of transfers under this Agreement be held by the European Commission to be invalid under the Data Protection Laws or be formally described by the Supervisory Authority as no longer providing for adequate protection for Personal Data under the Data Protection Laws, the Supplier will (at the option of the Customer):

- (a) immediately at no additional cost to the Customer put in place an alternative mechanism for transfers which has been prior approved in writing by the Customer having regard to the Data Protection Laws; or
 - (b) cease transfers of the Agreement Personal Data to the relevant recipient forthwith and procure that the relevant recipient immediately takes all actions as are necessary in order for the Supplier to comply with **clause 2.4.1.1**;
- 2.4.1.7 Ensure that every individual who is authorised to Process Agreement Personal Data (including for the avoidance of doubt employees and other staff working for Supplier or for any Approved Sub-Processor) has committed themselves to confidentiality (meaning that they are either subject to confidentiality obligations equivalent to those set out in the terms of this Agreement or that they are under an appropriate statutory obligation of confidentiality) and ensure that they will comply with this **clause 2**, be appropriately reliable, qualified and trained, and that they will only be permitted to have access to the Agreement Personal Data as necessary to perform their roles in relation to the provision of the Services;
- 2.4.1.8 Implement (and assist the Customer and the members of the Customer Group to implement) technical and organisational measures so as to ensure a level of security appropriate to the risk presented by Processing the Agreement Personal Data including the risk of varying likelihood and severity for the rights and freedoms of Data Subjects, and at a minimum to the standards prescribed by the Customer from time to time, and in particular from a Data Security Incident;
- 2.4.1.9 Notify the Customer immediately after becoming aware of any Data Security Incident, including the nature of the Data Security Incident, the categories and approximate number of Data Subjects and Agreement Personal Data records concerned, the name and contact details of the data protection officer or other contact point at the Supplier (or the relevant Approved Sub-Processor) where more information can be obtained, the likely consequences of the Data Security Incident, and any measure(s) taken or proposed to be taken to address the Data Security Incident and to mitigate its possible adverse effects, in each case taking into account the nature of the Processing and the information available to the Supplier, and where and in so far as it is not possible to provide all the relevant information at the same time, the information may be provided in phases without undue further delay, but the Supplier (and Authorised Sub-Processors, as applicable) may not delay notification under this **clause 2.4.1.9** on the basis that an investigation is incomplete or ongoing;
- 2.4.1.9a The Supplier must immediately after becoming aware of any 'near miss' notify the Customer.
- 2.4.1.9b The Supplier will and will procure that Authorised Sub-Processors will not notify any other person (such as regulators or data subjects) about Data Security Incidents or 'near misses' without the Customer's prior written consent.
- 2.4.1.10 Taking into account the nature of the Processing and at no additional cost to the Customer, assist the Customer and the members of the Customer Group in fulfilling its/their obligations under the Data Protection Laws, including in relation to:
- (a) (responding to requests for exercising Data Subjects' rights under the Data Protection Laws, including by appropriate technical and organisational measures, insofar as this is possible, and including the right to be informed, the right to have personal information corrected if it is inaccurate, the right to object to certain processing of personal information, the right to restrict processing of personal information, the right to have personal information erased (commonly known as 'right to be forgotten'), the right to have personal information corrected if it is inaccurate,

the right to object to certain processing of personal information, the right to restrict processing of personal information, the right to have personal information erased (commonly known as 'right to be forgotten'), the right to request access to personal information, the right to move, copy or transfer certain personal information (commonly known as 'data portability'), rights in relation to automated decision making including profiling, and the right to complain to the Supervisory Authority about infringements of the Data Protection Laws and for the avoidance of doubt in cases where a Data Subject has engaged the right to have personal information erased under the Data Protection Laws, the Supplier acknowledges and agrees that merely putting beyond use the Agreement Personal Data or suppressing the same will not amount to erasure so as to enable it to comply with this **clause 2.4.1.10(a)**;

- (b) (without prejudice to **clause 2.4.1.9**) documenting any Data Security Incidents (including the facts relating to the Data Security Incidents, their effects and the remedial action taken) and reporting any Data Security Incidents to the Supervisory Authority, any other Regulator and/or Data Subjects, including by taking into account the information available to the Supplier;
- (c) (without prejudice to **clause 2.4.1.9**) taking measures to address Data Security Incidents, including, where appropriate, measures to mitigate their possible adverse effects; and
- (d) conducting privacy impact assessments of any Processing operations and consulting with supervisory authorities, Data Subjects and their representatives in respect of the same; and

2.4.1.11 Promptly after the end of the provision of Services relating to Processing of the Agreement Personal Data (including following termination of this Agreement if that is when the provision of Services ends) and sooner at any other time at the written request of the Customer (provided the Customer is acting reasonably):

- (a) securely delete all Agreement Personal Data including by irrevocably, completely and permanently deleting the same, including from archives and back up facilities, as relevant, and in such a way that there shall be no ability to recover the same at any time from any medium, repository, or location whatsoever), or return to the Customer all Agreement Personal Data (and it shall be at the option of the Customer whether there is deletion or, in the alternative, return under this **clause 2.4.1.11(a)**);
- (b) (in the event that the Customer opts for return pursuant to **clause 2.4.1.11(a)**) securely delete any existing or remaining copies of the Agreement Personal Data (deletion having the same meaning as is set out above); and
- (c) promptly certify (via a director) when the exercise described in this **clause 2.4.1.11** has been completed provided always that if, following termination of this Agreement, the Customer has not within 30 days notified Supplier of its decision regarding the option between deletion or return under **clause 2.4.1.11(a)**, the Supplier will and will procure that the Approved Sub-Processors will securely delete all Agreement Personal Data (deletion having the same meaning as is set out above).

2.5 Information provision

- 2.5] The Supplier will, and will procure that Authorised Sub-Processors will and at no additional cost to the Customer:
- 2.5.1] make available to the Customer and the other members of the Customer Group all information necessary to demonstrate compliance with the obligations set out in this **clause 2**; and
 - 2.5.1.2 allow for and contribute to audits, including inspections, conducted by the Customer and/or the other members of the Customer Group or another auditor mandated by the Customer and/or the other members of the Customer Group; and
 - 2.5.1.3 allow for and contribute to audits, including inspections, conducted by the Supervisory Authority and provide all information necessary in response to any request from the Supervisory Authority in relation to the same, in each case which relates in whole or in part to the Agreement Personal Data; and
 - 2.5.1.4 without prejudice to **clauses 2.5.1.1, 2.5.1.2 and 2.5.1.3**, conduct an annual audit in respect of its processing of the Agreement Personal Data, its compliance with the Data Protection Laws including in relation to the Agreement Personal Data, and its compliance with this **clause 2**, and promptly thereafter supply the Customer with a copy of a written report in respect of the annual audit including the findings and outcomes relating to the same.

2.6 Indemnity

The Supplier will indemnify the Customer and each other member of the Customer Group and hold it and each of them harmless against all of the Liabilities (which includes all losses, damages and costs howsoever arising) suffered or incurred by it or them, in each case arising out of or in connection with any breach by the Supplier of any of its obligations under this **clause 2** (including any failure or delay in performing, or negligent performance or non-performance of, any of those obligations) including for the avoidance of doubt any breach by the Supplier which arises out of the actions or omissions of any of the Approved Sub-Processors.

2.7 Liability

The Supplier's liability for any breach of this **clause 2** and in respect of the indemnity at **clause 2.6** will be unlimited and for the avoidance of doubt all such liability will be outside of any cap(s) or limitation(s) as may be set out in the Agreement.

2.8 Termination for breach

A breach of this **clause 2** by the Supplier including for the avoidance of doubt any breach by the Supplier which arises out of the actions or omissions of any of the Approved Sub-Processors or of the Standard Contractual Clauses (as relevant) will be a material breach of this Agreement.

2.9 Conflict

The provisions of the Agreement shall at all times be subject to the Supplier's obligations under this **clause 2** and to the definitions under **clause 1** of this **Schedule 1**, and in the event of any conflict as between the Agreement and **clauses 1 and 2** of this **Schedule 1**, **clauses 1 and 2** of this **Schedule 1** shall prevail.

2.10 Interpretation of consent

Wherever under this **clause 2** the Customer's consent is required before the Supplier is permitted to do a particular act or thing, unless expressly provided otherwise, the Customer shall be entitled to give or withhold consent or make consent subject to conditions at its sole discretion.

2.11 Further assurance

The Supplier will execute all such documents and do all such acts or things as Customer may reasonably request from time to time in order for the Customer and the other members of the Customer Group to comply with its/their obligation(s) under the Data Protection Laws, in particular in respect of what is required in written terms between Data Controllers and Data Processors, including having regard to any updates to **clauses 1 and/or 2** of this **Schedule 1** which may be necessary from time to time by reason of formal guidance or codes of practice issued by the Supervisory Authority and which are relevant to the subject matter of this **Schedule 1**.

2.12 Description of Processing

2.12.1 The Supplier warrants and undertakes to ensure that its description of the Processing carried out on the Agreement Personal Data under this **Schedule 1** as is set out in the Annex to this **Schedule 1**, and as is completed in the first instance by the Supplier, is complete and accurate as at the date of the Supplier's signature on this **Schedule 1**.

2.12.2 The Customer reserves the right to review and amend the description of the Processing more particularly referred to in **clause 2.1.2.1** at its sole discretion.

2.13 Survival

The clauses in this **Schedule 1** shall survive termination of the Agreement.

Annex 1 – Details of Processing of Agreement Personal Data

The Processing of the Agreement Personal Data taking place under this Agreement includes that which is set out in the following description.

The subject matter of the Processing is:
Personal data provided in respect of potential and actual mortgage customers by Mortgage Intermediaries.

The duration of the Processing is:
As set out in this Agreement.

The nature and purpose of the Processing is:
In connection with the provision of the Services under the Mortgage Intermediary Agreement.

The type of Personal Data being Processed is:
May include full name, email addresses, home postal addresses, office/institution postal address, telephone, mobile phone numbers, job titles, employment details and background, professional background and training; gender, photographs, credit card, mortgage and bank account data and asset/liability data; government-issued identification, including passport numbers (for identification); date of birth (for identification); place of birth (for identification); loan details; marketing and advertising responses and preferences and other types of personal data (including for guarantors and non-borrowers) submitted by Customer to the Intermediary.

The categories of Data Subjects include:
Potential, new and existing borrowers, guarantors and non-borrowing occupiers.

The obligations and rights of the Data Controller(s) are:
As set out in this Agreement and in addition its/their obligations are prescribed under the Data Protection Laws.