<u>G Cloud – Equifax Supplemental Terms</u> <u>(“**Supplier Terms**”)</u>

<u>Part A – Supplier Terms</u>

1. DEFINITIONS

1.1 For the purposes of these Supplier Terms the following words and phrases shall mean as follows, unless expressly stated to the contrary:

“**Applicable Law**” means all laws, enactments rules, regulations, orders, regulatory policies, regulatory permits and licences, and any mandatory instructions or requests of a regulator, in each case which are in force from time to time, and in each case applicable to the activities of either party;

“**CRAIN**” means the Credit Reference Agency (CRA) Information Notice, the industry standard privacy information policy adopted by the leading UK CRAs (a copy of which can be found here: https://www.equifax.co.uk/crain), and as may be updated from time to time;

“**Exemptions**” means any exemptions under the DPA 2018 or other Data Protection Legislation, which exempt the requirement to provide fair notice to data subjects in relation to the processing of their Personal Data;

“**Information Services**” means the provision of access to data by the Supplier for the Permitted Purposes;

“**Input Data**” means any data provided by the Buyer to the Supplier to enable the Supplier to perform the Information Services;

“**Output Data**” means any information or data provided by the Supplier and received by the Buyer using the Information Services;

“**Permitted Purposes**” means the internal purposes for which the Information Services (including Output Data) may be used by the Buyer, as specified and defined in Part B to these Supplier Terms.

“**Product Rules**” Means those additional terms and conditions set out in Annex 1 (as applicable);

“**Search**” means a request for Output Data in respect of one person (or business) at one address, with each additional person (or business) or address then constituting an additional Search;

2. PERMITTED USE

2.1 The Buyer shall only use the Output Data;

2.1.1 in compliance with all Applicable Laws;

2.1.2 for the Permitted Purposes; and

2.1.3 otherwise in compliance with these Supplier Terms and any applicable Product Rules.

2.2 The Buyer must not:

2.2.1 resell or offer to resell any of the Output Data; or

2.2.2 disclose to any other person any of the Output Data, except:

2.2.2.1 when required to do so by law or any regulatory authority, including following a subject access request submitted by a consumer to whom the data relates; or

2.2.2.2 to the Buyer's personnel whose duties reasonably require such disclosure, on condition that the Buyer ensure that each such person to whom such disclosure is made, is informed of the Buyer's obligation of confidentiality and non-disclosure, and are subject to equivalent obligations.

2.3 The Buyer agrees that all Intellectual Property Rights in and to the "**Pre-Existing Materials**" being documentation (including drawings, plans, diagrams, pictures, disks or other device embodying information in any form), methodologies, processes, software, designs and development tools developed or used by the Supplier prior to the Start Date) and the Output Data are owned by (or licensed to) the Supplier and shall remain owned (or licensed) by the Supplier.

2.4 Subject to the Buyer complying (and continuing at all times to comply) with any conditions of this grant of licence, as from the Start Date grants to the Buyer a non-exclusive, revocable, non-transferable licence to use the Pre-Existing Materials and Output Data solely for the Permitted Purposes. Third party contractors or consultants of the Buyer may only use the Pre-Existing Materials and Output Data with the prior written consent of the Supplier.

3. AUTHENTICATION

3.1 Before providing any data to the Supplier or otherwise conducting a Search in relation to an individual consumer, the Buyer will ensure that it has undertaken all reasonable and appropriate checks to validate and authenticate the identity of the relevant consumer, except and to the extent that the purpose of conducting a Search is to undertake such checks.

3.2 The Buyer acknowledges that a failure to properly validate and authenticate a consumer may result in the use and/or disclosure of consumer data in breach of Applicable Law including the Data Protection Legislation, potentially requiring the involvement of the Financial Conduct Authority and/or the Information Commissioner's Office. Accordingly, to the extent that the Supplier or the Buyer becomes aware of or reasonably suspects that a consumer has not been properly authenticated or is not the person they purported to be, the Buyer will:

3.2.1 immediately notify the Supplier (which may be given via the Supplier) and provide all relevant details available to enable the Supplier to determine whether a notification to the Financial Conduct Authority and/or Information Commissioner's Office is required (a "**Notification**");

3.2.2 provide all reasonable assistance and co-operation requested by the Supplier in relation to a Notification or to otherwise investigate the matter.

4. ACCURACY

4.1 The Buyer acknowledges and agrees that:

4.1.1 the information forming part of the Output Data is provided to the Supplier by third parties over which the Supplier does not have control, in particular in relation to the accuracy or completeness of such information;

4.1.2 the volume and nature of the information on Supplier databases makes it impractical for the Supplier to verify the information;

4.1.3 if the Supplier attempted to verify the Output Data, the Supplier would only be able to offer the Information Services to the Supplier at significantly increased cost, which would in turn increase the costs paid by the Buyer; and

4.1.4 is not in any circumstances liable to any party for any loss or damage at all arising from any inaccuracies, faults or omissions in, or in the provision of, the Output Data unless caused by the Supplier's negligence or wilful default.

5. DATA PROTECTION AND TRANSPARENCY

5.1 Before providing any Input Data to the Supplier or otherwise conducting a Search in relation to an individual consumer, the Buyer shall:

5.1.1 notify the individual about whom a Search is made that their information will be disclosed to a credit reference agency, which may keep a record of that information and disclose it (and the fact that a search was made) to its other customers, including for the purposes of assessing the risk of giving credit and occasionally to prevent fraud, money laundering and to trace debtors;

5.1.2 make a copy of the CRAIN available to the individual so that they might understand how the credit reference agencies process their Personal Data; and

5.1.3 on request (which may be received directly or via the Supplier), provide a copy of the notification used to satisfy the obligations at clause 5.1.1 and 5.1.2 to the Supplier.

5.2 Where the Buyer is relying on an Exemption to process any Personal Data contained within any Input Data:

5.2.1 it is acknowledged that the Buyer and the Supplier may be exempt from providing fair notice in accordance with clause 5.1;

5.2.2 the Buyer shall notify the Supplier in writing of the relevant Exemption relied on, providing details as to why the Exemption applies;

5.2.3 the Buyer warrants that it can rely on the Exemption in relation to its processing of such Personal Data; and

5.2.4 the Buyer shall immediately inform the Supplier should it no longer be able to rely on the Exemption.

5.3 Unless an Exemption is being relied upon, the Buyer will ensure the correct Search type code, as notified by the Supplier to the Buyer, is used when conducting a Search, which the Buyer acknowledges is crucial to ensure that the resulting Footprint is accurate and reflects the Search undertaken and ay failure to use the correct Search type code may distort and create an inaccurate credit report for an individual or company, potentially impacting their ability to obtain credit or be verified. Where an Exemption is being relied upon, the Buyer acknowledges that a Footprint only visible to the Supplier will be created for the Supplier's audit purposes.

6. SECURITY AND AUDIT

6.1 The Buyer shall maintain adequate security measures to protect the integrity, security and confidentiality of all Output Data, including as a minimum by complying with the Supplier's security requirements and policies, as made available by the Supplier to Buyer from time to time.

6.2 The Buyer shall provide to the Supplier any information reasonably requested in order to assess whether the Buyer's use of the Information Services and Output Data is in compliance with these Supplier Terms.

Part B – Permitted Purpose

[The following Permitted Purposes should be deleted as appropriate for the Information Services being engaged].

Permitted Purpose	**Definition and Scope**
Credit Risk Assessment	Assessing the risk of granting credit to an applicant for consumer and/or business credit and directly relevant financial services.
Detecting Fraud	Identifying individual consumers or businesses making potentially fraudulent applications for credit and directly related financial services. Including undertaking (as

	applicable) address and bank account verification, employment status (and employer) checks, and Politically Exposed Person checks. In the context of this definition, "Fraudulent" means "fraud" as defined by the Fraud Act 2006 and any regulation, code of practice or government guidance (as amended or replaced from time to time).
Preventing Money Laundering	Identifying transactions and patterns of behaviour within individuals or businesses that seek to conceal the origins of illegally obtained money, typically by means of money transfers involving foreign banks or legitimate businesses as more specifically defined by the Proceeds of Crime Act 2002 and any regulation, code of practice or government guidance (as amended or replaced from time to time).
Debt Collection	Identifying the location (addresses) of debtors and assessing their ability to repay outstanding debts using a variety of legally available debt collection methods.
Individual ID Verification	Verifying the ID of individuals seeking to contract for goods and services, obtain credit and associated financial services, and apply for or take up an offer of employment.
Business ID Verification	Verifying the ID of a business entity (or an individual purporting to act on that businesses behalf) seeking to contract for goods and services, obtain credit and associated financial services.
Customer Management	To manage existing customer credit accounts by (i) setting credit limits, holds or facility increases; (ii) authorising individual transactions; and (iii) assess financial risks. Undertaking internal business analysis and research for the purposes of improving or developing products and service, provided that any Personal Data is anonymised or pseudonymised (as appropriate), and no information is used to profile or impact an individual consumer.
Employment ID, Credit and Fraud Risk Assessment	In relation to an employee or individual applying for a position of employment: (i) verifying their identity; (ii) assessing their creditworthiness (where permitted by Applicable Law); and/or (iii) detecting or preventing potential instances of fraud by undertaking (as applicable) address and bank account verification, employment status (and employer) checks, and Politically Exposed Person checks.

The Parties acknowledge and agree that none of the Permitted Purposes allow the use of Information Services for direct marketing purposes, as such term is defined in Data Protection Laws and Applicable Law, unless expressly stated to the contrary in the Call-Off Contract.

In relation to any of the Permitted Purposes (and for the avoidance of doubt), Information Services and Output Data may also be used where necessary to comply with Applicable Law; or to exercise or defend a legal right, including to defend against any consumer claim or complaint.

Annex 1 – Product Rules

[The following Product Rules should be deleted as appropriate for the Information Services being engaged].

Location tracing services and contact refresh – Product Rules – February 2023

For the purposes of the below product rules, "organisation" shall refer to the Customer.

1. Product Overview

a) The Equifax Tracing Services refers to the provision by Equifax of an individual's address, telephone number, email address or other contact details ("**Trace Data**") to assist in the tracing of an organisation's customers.

b) Equifax provides no warranty or guarantee that the Trace Data is accurate as it may not be current, and although the information is provided in good faith, Equifax is not in a position to check its validity. Therefore, no action should be taken by any organisation solely on the basis of the Trace Data alone, and organisations should undertake its own reasonable due diligence to verify that the information is relevant to the individual concerned.

2. DATA PROTECTION

a) In receiving and processing the Trace Data, the recipient organisation shall act as an independent Controller and will comply with its obligations under the Data Protection Laws.

b) Without prejudice to the generality of the above, the recipient organisation will ensure that it has a lawful basis to process the Trace Data and following receipt of the Trace Data, provides fair notice of its processing of the updated personal data the relevant individual within the period required under Data Protection Laws.

3. Rules of Use

a) The organisation will only use the Trace Data where it is necessary to contact an individual in relation to any of the following:

   a. debts owed by the individual to the organisation or a third party for which the organisation is acting;
   b. products or services the individual currently receives (or has previously received) from the organisation, and such contact is necessary to provide that individual with one or more of the following:
      i. necessary service updates, which do not unfairly prejudice the individual;
      ii. information in relation to assets or monies due to the individual; or
      information in relation to any other benefits due to the individual,

provided that at all times, the organisation **does not** use the Trace Data for any direct marketing purposes (as such term is defined in the Data Protection Laws), including (for the avoidance of doubt) any communications requesting permission to send direct marketing, any offers of product or service upgrades or other cross selling, without having first obtained the consent of the individual to use the Trace Data for this purpose.

b) To the extent that there is a change in applicable laws (including the Data Protection Laws) or a regulator publishes guidance, which indicates that provision of Trace Data is (or will be) unlawful, Equifax may immediately suspend or terminate the organisation's access to Trace Data by written notice, explaining the issue giving rise to such suspension or termination, which the parties will discuss in good faith.

BT OSIS END USER TERMS/PRODUCT RULES

These BT OSIS Terms shall only apply where the Customer receives BT OSIS Data as part of a QCB (as such term is defined above).

1. For the purposes of these BT OSIS Terms, the following definitions shall apply:

“BT”	shall mean British Telecommunications plc;
“BT OSIS Data”	the name, address and telephone number of a consumer or business;
“BT Marks”	shall mean registered or unregistered trademarks and service marks, house marks and marks of ownership, trading names, brand names, distinctive colour schemes, devices, styles, emblems and other manifestations associated with BT;
“You” or “Your”	shall mean the Licensee’s customer;
“Licensee”	shall mean Equifax Limited.

2. These BTOSIS Terms shall apply only to the extent that You receive BT OSIS Data from the Licensee.
3. In relation to Your receipt and use of BT OSIS Data, You shall:

a. comply with all applicable laws and codes of practice including those in relation to data protection and privacy of information;
b. use all reasonable endeavours to prevent any unauthorised disclosure of any BT OSIS Data and keep it appropriately secure and confidential; and
c. only use or process any of BT OSIS Data for Your own internal purposes or, in the alternative, for a single use for a single specific person who is Your customer.

4. To the extent that any complaint is made which relates to Your use of the Information, You shall assist BT and the Licensee in investigating the complaint and shall take such steps as are reasonably necessary to remedy the complaint as soon as practicable.
5. You shall not:

a. distribute, publish or display any material amount of the BT OSIS Data by any means, except as otherwise permitted by these BT OSIS Terms;
b. export or permit the export of the BT OSIS Data to a country which is not within the UK or European Economic Area, without the prior written express consent of the Licensee and/or BT;
c. have any rights to use the BT Marks and shall not make reference to BT or any BT product or service in any promotional or marketing advertising, communications, literature or packaging; and
d. alter any copyright or other intellectual property right acknowledgement or confidentiality marking incorporated into or applied to the BT OSIS Data and/or documentation owned by BT.

6. You acknowledge that BT OSIS Data only provides the surname of an individual and therefore does not, on its own, meet the full name match threshold outlined in the HM Treasure approved Joint Money Laundering Steering

Group 'JMLSG' (AML industry) guidelines for use as part of anti-money laundering checks.

DOW JONES PRODUCT RULES

The Customer shall comply with the following end user licence, which Equifax is required to flow down to all recipients of DOW Jones data:

DOW JONES END USER LICENCE

The terms set out in this End User Agreement ("**EUA**") apply to the Dow Jones Data.

In this EUA, the following terms shall have the following meanings:

"**Customer**" means the recipient of Dow Jones Data from Equifax.

"**Dow Jones Data**" means personal data (full name, maiden name or AKAs, place and date of birth, country of residence and country of citizenship, occupation and information on additional roles and the relationship (if applicable) to a public figure) compiled and maintained by Dow Jones on data subjects, including Politically Exposed Persons (PEPs) and Special Interest Persons (SIPs) which includes individuals due to his/her prominence in the news owing to his/her involvement in selected criminal activity:

"**Dow Jones**" means Factiva Limited, a company incorporated in England and Wales under number 3773253 and with registered address at The News Building, 1 London Bridge Street, SE1 9GF London, England, acting on behalf of Dow Jones & Company, Inc. and any of its affiliated companies; and

"**Permitted User**" ***means*** an individual authorised to access and use the Dow Jones Data and who is either: (a) an individual employee of the Customer; (b) an individual performing the functions of an employee on a temporary basis, independent contractor or consultant, in each case who is performing work for the Customer; or (c) an individual working for a company engaged by the Customer ("**Third Party Contractor**") to perform research using the Dow Jones Data on the Customer's behalf, for the benefit of the Customer provided that the Customer: (i) assumes full responsibility and liability for the acts and omissions of all Permitted Users and the Third Party Contractor, as if such acts and omissions were committed or made by the Customer; and (ii) ensure that the Third Party Contractor and all Permitted Users use the passwords (provided by the Customer) only on a dedicated basis for the Customer.

1. Licence

1.1 **Equifax** grants to the Customer a non-exclusive, non-transferable, non-sub licensable, non-assignable licence to use the Dow Jones Data subject to the terms and conditions of this EUA and the agreement under which it is appended ("**Agreement**").

1.2 The Dow Jones Data contains information derived from publicly available sources, and will be regularly up-dated by **Equifax** as updates are received from Dow Jones. Dow Jones retains control and ownership of the form and content of the Dow Jones Data, and although Dow Jones may alter the Dow Jones Data from time to time, its fundamental nature will not be changed. The Customer and Permitted Users will not, under the Agreement and this EUA acquire any ownership rights in the Dow Jones Data.

2. Terms of use

2.1 The Customer and Permitted User shall use the Dow Jones Data in strict compliance with applicable laws and regulations within the jurisdictions in which it accesses and uses the Dow Jones Data. The Customer shall ensure that the Dow Jones Data shall only: (a) be accessed by Permitted Users; and (b) be used for the legitimate interests of the Customer and particularly for the purposes of assisting in complying with legal duties and regulations which apply to the Customer such as due diligence, anti-money laundering, "know your customer" compliance or similar regulatory screening obligations.

2.2 Except to the extent permitted or required for the Customer's permitted use under section 2.1, the Customer and/or Permitted Users shall not: (a) reproduce, distribute, display, sell, publish, broadcast or circulate the Dow Jones Data to any third party, nor make the Dow Jones Data available for any such use; or (b) create or store in electronic form any library or archive of the Dow Jones Data save that, and notwithstanding anything to the contrary, the Customer shall be entitled to retain copies of the Dow Jones Data necessary for archival, regulatory and/or compliance purposes. The Customer's right to retain such copies as set forth above shall survive termination/expiration of this EUA provided that it no longer actively uses the Dow Jones Data.

2.3 The parties agree that upon termination of the provision of the Dow Jones Data and unless otherwise provided by subject applicable legal or regulatory restrictions, the Customer shall return or destroy all Dow Jones Data together with any copies, and certify in writing to **Equifax** the completion of this process. In the case where the Customer is required by law or regulation to keep copies of some of the Dow Jones Data, the Customer guarantees the confidentiality of the Dow Jones Data and will not use the Dow Jones Data for any other purpose.

3. Data Protection principles

3.1 The Customer shall comply with all applicable laws and regulations within the jurisdictions, in which the Customer processes the Dow Jones Data, and the Data Processing Principles set out below. The Customer acknowledges that an individual who is included in the Dow Jones Data (an "**Individual**") can enforce in his/her country of establishment this provision against the Customer with respect to its personal data. Any person acting under the authority of the Customer, including a data processor, shall be obligated to process the Dow Jones Data only on instructions from the Customer and on terms no less stringent than those set out in the Data Processing Principles below.

3.2 Upon reasonable request of **Equifax**, the Customer will submit its data processing facilities, data files and documentation needed for processing to review, audit and/or certification by **Equifax** (or any independent or impartial inspection agents or auditors, selected by **Equifax** and not unreasonably objected to by the Customer) to ascertain compliance with the warranties and undertakings in this EUA, with reasonable notice and during regular business hours. Such request will be subject to any necessary consent or approval from a regulatory or supervisory authority within the country of the Customer, which consent or approval the Customer will attempt to obtain in a timely fashion.

4. Warranties

Equifax shall make reasonable efforts to ensure that the Dow Jones Data is up to date. While **Equifax** will use its reasonable efforts to ensure that the Dow Jones Data is complete, **Equifax** cannot warrant that the Dow Jones Data includes a complete or accurate archive of every public figure or their associates in each country. Except as specified in this EUA all express or implied representations, warranties, conditions and undertakings in relation to the provision of the Dow Jones Data are excluded.

5. Customer Information

Please note that **Equifax** will report to Dow Jones the name of the Customer and the number of name queries screened against the Dow Jones Data, but not its nature. This information will only be used by Dow Jones to verify the relevant usage of the Dow Jones Data and the payments due and payable to Dow Jones in this respect. Dow Jones shall not disclose such information to any third party, other than to members of its group companies, or use them for any other purpose whatsoever and will treat this information as Confidential Information.

DATA PROTECTION PRINCIPLES

1. **Purpose limitation**: Personal Data may be processed and subsequently used or further communicated only for the following purposes: (a) assisting in complying with legal duties and regulations which apply to the Customer; (b) performing a statutory role as a Governmental organization; or (c) performing law enforcement duties. If the Customer is processing special categories of data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life ("Sensitive Data"), it shall only process it for the purpose of preventing fraud or a similar crime (the "Purposes").

2. **Personal Data quality and proportionality**: Personal Data must be accurate and, where necessary, kept up to date. Personal Data must be adequate, relevant and not excessive in relation to the purposes for which they are transferred and further processed.

3. **Transparency**: Individuals must be provided with information necessary to ensure fair processing (such as information about the purposes for processing and about the transfer), unless such information has already been given by **Equifax**.

4. **Security and confidentiality**: Technical and organisational security measures must be taken by the Customer that are appropriate to the risks, such as against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, presented by the processing. This obligation shall not apply where the Customer is accessing services via the hosted solutions of **Equifax**.

5. **Rights of access, rectification, deletion and objection**: An Individual must, whether directly or via a third party, be provided with the Dow Jones Data about him/her that an organisation holds, except for

requests which are manifestly abusive, based on unreasonable intervals or their number or repetitive or systematic nature, or have been dismissed by the relevant data protection authorities, or when doing so would be likely to seriously harm the interests of the Customer or other organisations dealing with the Customer and such interests are not overridden by the interests for fundamental rights and freedoms of the Individual. The sources of the Dow Jones Data need not be identified when this is not possible by reasonable efforts, or where the rights of persons other than the Individual would be violated. An Individual must be able to have the Dow Jones Data about him/her rectified, amended, or deleted where it is inaccurate or processed against these principles. If there are compelling grounds to doubt the legitimacy of the request, **Equifax** or the Customer may require further justifications before proceeding to rectification, amendment or deletion. Notification of any rectification, amendment or deletion to third parties to whom the Dow Jones Data has been disclosed need not be made when this involves a disproportionate effort. The burden of proof for any refusal rests on the Customer or **Equifax**, and the Individual may always challenge a refusal before the relevant data protection authorities.

6. **Sensitive Data**: The Customer shall take such additional measures (e.g. relating to security) as are necessary to protect such Sensitive Data in accordance with its obligations under the Agreement or this EUA.

7. **Automated decisions**: For purposes hereof "automated decision" shall mean a decision by **Equifax** or the Customer which produces legal effects concerning an Individual or significantly affects an Individual and which is based solely on automated processing of Dow Jones Data intended to evaluate certain personal aspects relating to him/her, such as his/her performance at work, creditworthiness, reliability, conduct, etc. The Customer shall not make any automated decisions concerning Individuals, except when: (a) (i) such decisions are made by the Customer in entering into or performing a contract with the Individual, and (ii) the Individual is given an opportunity to discuss the results of a relevant automated decision with a representative of the parties making such decision or otherwise to make representations to that parties; or (b) where otherwise provided by applicable laws or regulations.