



Notice for Consumers

About HubSolv

HubSolv Ltd treat our customers' privacy very seriously and we want you to feel confident and comfortable about how we process your personal data. This notice outlines how your data is processed by HubSolv in accordance with legal mandates. We are a Data Controller and adhere to these procedures as defined by the Data Protection Legislation.

We act as a technology service for advisors and providers of debt solutions who offer debt advice to public consumers. We do not directly provide or administrate debt solutions to the public.

Advisors that use our services may provide and/or administer popular debt solutions in England, Scotland, and Wales including Individual Voluntary Arrangement, (IVA), Debt Management Plan (DMP), Debt Arrangement Scheme (DAS), Protected Trust Deed (PTD) and Sequestration. An FCA-recognised Advisor or Provider can provide you with detailed information on the above debt solutions and their differences.

Our role at HubSolv Ltd is to improve the efficiency and overall quality of debt solutions offered to consumers by providing a case management platform for advisors. We also offer a client portal that allows consumers to provide further information surrounding their overall financial health to communicate directly with their chosen advisor. We have no say or influence over the outcome of a particular customer's debt solution.

Our postal address is: - HubSolv Ltd, 3rd Floor, The Reel House, 7 West Regent Street, Glasgow G2 1RW. This is the registered contact and firm information for HubSolv Ltd.

Or you can email – office@hubsolv.com

This policy outlines the accessibility and collection of your personal data in relation to TransUnion (the "Provider"). "References to "TransUnion" in these terms and conditions means: TransUnion International UK Limited (company number 3961870), authorised and regulated by the Financial Conduct Authority under number 737740, whose registered office is at One Park Lane, West Yorkshire, LS3 1EP. Authorisation can be checked on the Financial Services Register at www.fca.org.uk.

For Consumers

Your Advisor will decide if they wish to use our services to help identify the best debt solution. They may do some or all of the following: -

- 1) Access your Credit Report;
- 2) Access your Bank Transaction data;
- 3) Access your wage slips, proof of identification, and all other documentation related to your overall financial health;



Privacy Notice for Consumers

Your **personal data** that we would like to collect and subsequently process:

- 1) Name, address, contact details, date of birth, dependents, and employment details;
- 2) Financial information such as: income, expenditure, assets, and debts;
- 3) "Other" category data such as: health information related to your income, vulnerability if applicable, and ability to manage your debts.

The **source** of obtaining this data, if not obtained directly from HubSolv Ltd, will be one of the following:

- 1) Advisor;
- 2) Credit Reference Agency;
- 3) DVLA Search

The personal data we collect will be used for the **following purposes**:

- 1) Credit Reports - will be held for access by your appointed advisor. To achieve this the data provided by you will be provided to the following Credit Reference Agencies to assist with identity verification, prevention of fraud/money laundering, and any other uses that may be mutually agreed upon by the parties from time to time;
 - a) TransUnion Information Group. You can view the TransUnion Bureau Privacy Notice at <https://www.transunion.co.uk/legal/privacy-centre?#pc-bureau>
 - b) Equifax Limited. You can view the Equifax Privacy Notice at https://www.equifax.co.uk/privacy/en_gb/
- 2) Bank Transaction Data – HubSolv Ltd are directly authorised by the FCA to access this information, and this will be held for access by your appointed advisor.

Consent

Advisors will obtain your consent to process your data specifically for the purposes identified. Consent is required for HubSolv Ltd to process both types of personal data, but it must be explicitly given. Where your advisor asks for sensitive personal data, they will always tell you why and how the information will be used.

Where we rely on your consent you may withdraw it at any time by contacting your advisor who will notify us immediately to remove the data from the system.

Retention period

1. Credit Reports - will be stored for 30 days and then deleted.
2. Banking Transaction Data - will be stored for as long as we have your consent.

Your Rights

At any point whilst we are in possession of, or processing your personal data, you, the data subject, have the following rights:

- Right of access – you have the right to request a copy of the information that we hold about you.
- Right of rectification – you have a right to correct data that we hold about you that is inaccurate or incomplete.
- Right to be forgotten – in certain circumstances you can ask for the data we hold about you to be erased from our records. Please bear in mind the retention periods mentioned above.
- Right to object/restriction of processing – if you wish us to stop, pause or restrict processing your data please contact us via your advisor or follow the instructions on the Consent Withdrawal Form.
- Right of portability – we can download the data we hold about you into a machine-readable format. Please contact us via your advisor if you require this.
- Right to complain: in the event that HubSolv Ltd refuses your request under rights of access, we will provide you with a reason as to why. You have the right to complain as outlined in the clause below.

All of the above requests will be forwarded on should there be a third party involved in the processing of your personal data.

Privacy Notice for Customers

Data protection

The parties agree that the Customer is a Controller (as defined in the Data Protection Legislation) and that the Provider is a Processor (as defined in the Data Protection Legislation) for the purposes of processing Protected Data pursuant to this Agreement. The Customer shall at all times comply with all Data Protection Legislation in connection with the processing of Protected Data. The Customer shall ensure all instructions given by it to the Provider in respect of Protected Data (including the terms of this Agreement) shall at all times be in accordance with Data Protection Legislation. Nothing in this Agreement relieves the Customer of any responsibilities or liabilities under any Data Protection Legislation.

- 1) The Provider shall process Protected Data in compliance with the obligations placed on it under Data Protection Legislation and the terms of this Agreement.
- 2) In the event that the Provider processes any Protected Data on behalf of the Customer under this Agreement the Provider undertakes:
 - (a) except as required by law, to act only on reasonable and lawful instructions from the Customer in relation to the processing of Protected Data, to inform the Customer if the Provider believes that any instruction received from the Customer is likely to infringe Data Protection Legislation, in which case the Provider may cease to provide the relevant Service, and not to process Protected Data for any purpose other than as required by this Agreement;
 - (b) taking account of the state of technical development and the nature of the processing, to put in place appropriate security measures (both technical and organisational) against unlawful or unauthorised processing of, and against accidental loss or destruction of, or damage to, Protected Data;
 - (c) that any of its employees who will have access to Protected Data are under appropriate confidentiality obligations in respect of the Protected Data, have undergone data protection training and are aware of their obligations under the Data Protection Legislation;
 - (d) at the Customer's cost, to provide reasonable assistance on request to the Customer in complying with the rights of data subjects and with the Customer's statutory obligations under the Data Protection Legislation insofar as the foregoing relate to Protected Data;
 - (e) at the Customer's cost to provide the Customer with such information as the Customer may reasonably require to satisfy itself that the Provider is complying with its obligations under the Data Protection Legislation;
 - (f) to notify the Customer immediately if it receives a complaint, notice or any other communication concerning the Provider's processing of Protected Data;

- (g) at the Customer's cost, allow the Customer to appoint an independent auditor to audit and inspect the Provider's compliance with this Clause 14.3 and Clause 14.4. Such audit may occur once per calendar year, unless the Customer can demonstrate that it has genuine suspicion that the Provider has breached its obligations in this Clause 14. Such an audit shall be carried out during business hours and the Customer shall provide at least 30 Business Days' notice of any such audit, unless the Customer can demonstrate that it has genuine suspicion that the Provider has breached its obligations in this Clause 14 in which case the Customer shall provide at least 2 Business Days' notice of any such audit;
 - (h) to notify the Customer without undue delay and in writing of any personal data breach in respect of Protected Data;
 - (i) not to transfer the Personal Data to a country outside the European Union without the authorisation of the Customer unless the relevant territory ensures an adequate level of protection or appropriate standard contractual clauses approved by the EU have been put in place or other appropriate safeguards have been implemented;
 - (j) except as required by law, after termination of this Contract return to the Customer or destroy, at the request of the Customer at the Customer's cost, all Customer Personal Data in the possession of the Provider; and
 - (k) to restrict any processing immediately as directed by the Customer.
- 3) The Customer authorises the appointment of sub-processors. The Provider shall:
- (a) inform the Customer of changes to the identity of its sub-processors;
 - (b) appoint the relevant sub-processor under a written contract containing materially the same obligations as under Clause 14.3 or Article 28 of the General Data Protection Regulation (including those relating to sufficient guarantees to implement appropriate technical and organisational measures); and remain fully liable to the Customer under this Agreement for all the acts and omissions of each such sub-processor as if they were its own.

Privacy Notice for Customers

Confidentiality and publicity

- 1) The Provider will:
 - (a) keep confidential and not disclose the Customer Confidential Information to any person save as expressly permitted by this Clause 15;
 - (b) protect the Customer Confidential Information against unauthorised disclosure by using the same degree of care as it takes to preserve and safeguard its own confidential information of a similar nature, being at least a reasonable degree of care; and
- 2) The Customer will:
 - (a) keep confidential and not disclose the Provider Confidential Information to any person save as expressly permitted by this Clause 15;
 - (b) protect the Provider Confidential Information against unauthorised disclosure by using the same degree of care as it takes to preserve and safeguard its own confidential information of a similar nature, being at least a reasonable degree of care.
- 3) Confidential Information of a party may be disclosed by the other party to that other party's officers, employees, agents, insurers and professional advisers, provided that the recipient is bound in writing to maintain the confidentiality of the Confidential Information disclosed.
- 4) The obligations set out in this Clause 15 shall not apply to:
 - (a) Confidential Information that is publicly known (other than through a breach of an obligation of confidence);
 - (b) Customer Confidential Information that is in possession of the Provider prior to disclosure by the Customer, and Provider Confidential Information that is in possession of the Customer prior to disclosure by the Provider;
 - (c) Customer Confidential Information that is received by the Provider, and Provider Confidential Information that is received by the Customer, from an independent third party who has a right to disclose the relevant Confidential Information; or
 - (d) Confidential Information that is required to be disclosed by law, or by a governmental authority, stock exchange or regulatory body, provided that the party subject to such disclosure requirement must where permitted by law give to the other party prompt written notice of the disclosure requirement.

- 5) Neither party will make any public disclosure relating to this Agreement (including press releases, public announcements and marketing materials) without the prior written consent of the other party.

Complaints

In the event that you wish to make a complaint about how your personal data is being processed by HubSolv Ltd or how your complaint has been handled, you have the right to lodge a complaint directly with the supervisory authority.

In order to lodge a formal complaint with HubSolv Ltd, the Consumer/Customer is asked to contact HubSolv Ltd using the information given in the chart below. HubSolv Ltd are available via the office phone line from the working hours of 09:00-17:30 from Monday to Friday, and are also available to receive complaints via email at the domain listed below. Complaints are reviewed by the Privacy & Data Manager and the Directors of HubSolv Ltd and are actioned within one (1) working day of receipt.

Contact and

The details for each of these contacts are:

	Supervisory Authority Contact Details	GDPR Owner Contact Details
Contact Name:	The Information Commissioner's Office – Scotland	Privacy & Data Manager, HubSolv Ltd
Address Line 1:	45 Melville Street	The Reel House
Address Line 2:		3/F 7 West Regent Street
Address Line 3:	Edinburgh	Glasgow
Postcode:	EH3 7HL	G2 1RW
Email:	scotland@ico.org.uk	office@hubsolv.com
Contact Number:	0303 123 1115	0141 404 9399

Customer Mandatory Conditions

This section will outline the policies and procedures in which HubSolv Ltd (the Distributor) expects the Advisor in question (the Customer) to communicate and distribute information to the debtor (the Consumer). The following items must be met

when the Customer is liaising with the Consumer to ensure that data sharing is compliant.

The Customer shall obtain the Consumer's Consent prior to requesting the Limited Subject Access Request Data (known furthermore as "LSAR Data"), and if the Consumer later withdraws the Consent, the Customer shall immediately delete any LSAR Data it holds in relation to that Consumer and shall cease providing the Consumer with Client Services which rely upon any LSAR Data. By submitting requests to the Distributor for LSAR Data under a Client Agreement, the Customer agrees that it has in place the relevant and up-to-date Consent.

The Consent obtained from the Consumer shall as a minimum:

1. provide the Consumer with a clear and concise description of what a credit report is, how the data requested from

TransUnion is going to be used and set out an alternative route of application for the relevant Client Service if the Consumer does not wish for LSAR Data to be requested from TransUnion on its behalf;

2. make clear to the Consumer which data items contained in the credit report the Customer is requesting from TransUnion,

The Customer shall retain records of the Consent(s) given by each Consumer and shall allow TransUnion to review these records promptly upon request. The Input and the Consent shall be collected by the Customer from the Consumer contemporaneously with the submission of the Input to TransUnion (via the Distributor).

If TransUnion informs the Customer (via the Distributor) that a Consumer has failed Authentication, the Customer shall offer that Consumer an alternative route of application for the relevant data (such as asking the Consumer to obtain their credit report via the Online LSAR route or manually providing details of their current and previous credit products).

Subject to the Customer's obligations under applicable Regulatory Requirements, the Customer shall delete all copies of a Consumer's LSAR Data from its systems as soon as the Service has been completed and the Customer shall provide TransUnion with copies of its data retention policies and procedures on request.

The Customer shall ensure that the methods it uses to provide any Services using the LSAR Data do not result in the LSAR Data being rendered inaccurate or misleading.

If the Customer receives a request from or on behalf of either (i) a Regulator, (ii) a Consumer or (iii) a Customer for access to or copies of any personal data which comprises or is derived from the Output (including any request under Article 15 of the GDPR), the Customer shall (except to the extent prohibited by law) inform TransUnion (via the Distributor) of such event and provide details of the request to

TransUnion (via the Distributor) (having removed any personal data contained in such request) as soon as reasonably practicable.

The Customer shall not issue any promotional or marketing material or publish any website content in connection with the Online LSAR or use TransUnion's name, trade marks or intellectual property without the prior written approval of TransUnion. In order to deal with the sensitivities that some data subjects may have regarding the use of their data for ID verification purposes, the Customer shall offer alternative methods by which a data subject can verify their identity and shall not discriminate against a data subject because of their refusal to use or permit the use of electronic ID verification systems.

The Customer shall acknowledge that LSAR Data shall leave a footprint on the Consumer's credit file, which is not visible to lenders, but will be visible to the Consumer and this footprint will either read as having been made by the Distributor or will read as having been made by the Distributor on the Customer's behalf (at TransUnion's sole discretion).

The Customer will procure that any Output provided to it is only used for the Permitted Purpose, which is heretofore defined as; the means by which to both verify the Consumer's credit history and subsequently qualify the Consumer (via the Customer's best and most accurate knowledge) for a debt solution.

The Customer will keep any Output provided to it by the Distributor confidential;

The Customer shall comply with the provisions of the Data Protection Legislation and all other applicable Regulatory Requirements in respect of the Input, Output and Client Services, heretofore defined as;

- a. "Input" is to be defined as the Customer's request (via the Distributor) to the Consumer that they will have their personal data accessed by the Customer;
- b. "Output" is to be defined as the personal data that the Customer returns to the Consumer (via the Distributor);
- c. "Client Services" is to be defined as the full-cycle journey from start to finish whereby the Consumer's personal data is obtained by the Customer via the Distributor, and returned to both the Customer and the Consumer.

The Customer shall at all times implement and maintain information security standards in respect of the Output which are in all material respects equivalent to or exceed the standards afforded by the Distributor Minimum Security Standards (as amended from time to time);

The Customer shall not under any circumstance sell, transfer, distribute or otherwise make any Output provided to it available to, or use the Output on behalf of, any other third party;

The Customer will procure that after the Output has been used once in the

assessment, the Output will not be accessed thereafter other than for audit purposes;

The Customer shall not assign, transfer or otherwise make over any part of the Customer Agreement without TransUnion's prior written consent;

Subject to the Customer being given reasonable prior written notice, the Customer shall permit the Distributor and TransUnion to have reasonable access during the Customer's normal business hours to the Customer's relevant premises and relevant operations for the sole purpose of ensuring that the Customer is complying with its obligations under the Customer Agreement;

The Customer shall not (without the prior written consent of TransUnion) sub-contract the performance of any of its obligations under the Customer Agreement and shall not (without the prior written consent of TransUnion) assign or transfer any part of the Customer Agreement;

TransUnion will have the right to enforce the terms and conditions referred to in this the applicable Service Schedule in accordance with the Contracts (Rights of Third Parties) Act 1999;

The Customer shall acknowledge and agree that the data comprised within the Output is based on information provided to TransUnion by third parties over whom TransUnion has no control and that therefore TransUnion gives no warranties or representations as to the accuracy or the completeness of the Output.

The Customer shall acknowledge and agree that TransUnion makes no warranties or representations as to the suitability of the Output for any particular purpose; that the Customer is responsible for satisfying itself that the Output is suitable for any use (within the scope of the Customer Permitted Purpose) and that TransUnion recommends that the Customer does not use the Output as the sole basis for any business decision.

Consumer Mandatory Conditions

The Distributor shall procure that each Customer includes the following provisions in each Consumer Agreement entered into between a Customer and a Consumer:

- 1.1 The Consumer Agreement shall expressly state that certain elements of the Services utilise data provided by TransUnion ("TransUnion Provided Data") and that as such, the Customer will need to share data collected from the Consumer with TransUnion via the Distributor (and its subcontractors) in order to provide the TransUnion Provided Data.
- 1.2 The Customer shall make clear in the Consumer Agreement that the source of the LSAR Data utilised in the provision of the Services is TransUnion.

- 1.3 The Customer shall make the Consumer aware of how its data will be used by the Customer (and by TransUnion in relation to TransUnion Provided Services) with a privacy notice that make reference to such processing which meets the requirements of the Data Protection Legislation.
- 1.4 The Customer shall make the Consumer aware that in the event of a query or dispute in connection with the Services it should contact the Customer or the Distributor in the first instance; and that if its query or complaint relates to the data that TransUnion holds and the Customer is not able to resolve such query or dispute, the Customer may refer the query or dispute to TransUnion.
- 1.5 The Customer shall include the following terms in the Consumer Agreement:
 - (a) the Consumer will be required to successfully pass an authentication process before the Customer will be provided with the TransUnion Provided Data. Not all Consumers will successfully pass authentication and neither the Customer nor TransUnion are required to notify the Consumer why it has not been successfully authenticated, but one reason for this may be that, at the time the Customer requests the TransUnion Provided Data, TransUnion has been unable to match the Consumer's personal details to the correct credit profile in its database;
 - (b) the Customer will only be provided with TransUnion Provided Data in respect of Consumers that are over 18 years of age and who live in the UK, the Channel Islands or the Isle of Man.
 - (c) the Customer confirms that the person utilising the Services and providing the Consent is the individual Consumer and they are not doing so on behalf of a third party (whether as agent or representative on behalf of, or as a service provider to, or otherwise);
 - (d) TransUnion shall use its reasonable efforts to verify the accuracy of the information provided as part of TransUnion Provided Data. However, TransUnion cannot guarantee that it is completely accurate as some of this information comes from other businesses, which get the information from other sources themselves such as the electoral register, insurance companies or financial institutions. Neither TransUnion, nor any other third parties used to provide the TransUnion Provided Data have any control over the content of such information and are not responsible if it turns out to be inaccurate;
 - (e) any TransUnion Provided Data, or information derived from the TransUnion Provided Data, that is provided to the Customer is provided for guidance and information only. The fact that a Consumer has a good credit score does not mean that a lender, credit card company or other provider of financial services products will accept their application, and they have their own acceptance criteria. Also, a credit score does not take into consideration affordability issues which are also considered by financial services/credit providers;
 - (f) the Customer reserves the right to suspend access to Services, any TransUnion Provided Data or any information derived from the TransUnion Provided Data if at any time TransUnion or the Customer considers that there is or is likely to be a breach of security; the Customer is misusing Services, any TransUnion Provided Data or any information derived from the TransUnion Provided Data (meaning use thereof in a way which is not permitted or is fraudulent); or the use of Services, any TransUnion Provided

Data or any information derived from the TransUnion Provided Data is in any way detrimental to the Customer or TransUnion;

(g) the Consumer acknowledges and agrees that all intellectual property rights in the TransUnion Provided Data or any information derived from the TransUnion Provided Data and all aspects of them shall be owned by TransUnion and/or its licensors.

1.6 The Customer shall draw to the Consumer's attention the following provisions as part of the Consumer Agreement:

(a) the request for LSAR Data shall leave a footprint on the Consumer's credit file, which is not visible to lenders, but will be visible to the Consumer and this footprint will either read as having been made by the Distributor or will read as having been made by the Distributor on the Customer's behalf (at TransUnion's sole discretion).

(b) in order to allow the Customer to access the LSAR Data as part of the Services, the Consumer is submitting a request under section 15 of the GDPR (or any successor legislation) to TransUnion (via the Distributor).