

DATA PROTECTION INFORMATION LEAFLET - IVA

Introduction

As part of delivering our service to you we will collect and process confidential information about you and your circumstances. We will comply with data protection law and keep all confidential information we receive from you or about you secure.

. We will need you to keep us updated throughout the life of your IVA of any changes in your situation. We will as part of delivering our service to you to share all the data we hold about your financial situation with your creditors and in some instance the Insolvency Service. We will provide information to your creditors and their agents in order for us to prepare your IVA in readiness for your creditors approval and the appointment of your Nominee. All the information we provide to your creditors will be objective, complete and accurate. Your fullest co-operation will be necessary for us to fully achieve this.

1. Your creditors and keeping the information we hold about you up to date

As a minimum at the outset of your instructions and subject to your circumstances we will ask you for updated personal and financial information. This is so that when your proposal is drafted by your Insolvency Practitioner your creditors have up to date and accurate information including your personal details

If approved by your creditors during the course of your IVA your Insolvency Practitioner will be required to provide up to date information to your creditors. Your co-operation will be required in order that they can provide meaningful updates in relation to your circumstances to your creditors as the Regulatory rules require them to do so.

The client authority form that we will ask you to sign so that we can process your personal data will set out the creditors from whom we will seek and share your personal information with. If necessary we will update this from time to time.

2. Collection and processing of your personal data.

We will collect personal information about you both directly from you and from your creditors as authorised by your signed Client Authority Form.

We will collect and process your personal data in order for us to provide our services to you, and in particular to:

- Collate all the information required for the transfer of your paperwork to your Insolvency Practitioner
- We will advise you on the suitability of an IVA to your circumstances and any alternatives that may become available to you.
- We will record all telephone calls you (or any third party you authorise to act on your behalf) make and/or receive from us concerning your IVA

updating/providing information to creditors and their appointed representatives be it collection agencies or Solicitors.

- We will record all telephone calls we make or receive from your creditors
- Provide information to Enquiry Agents if we lose touch with you
- Updating/providing information to the Court should that be necessary if any legal action is commenced against you.
- Providing information to enquiry agents if we lose touch with you
- Outsourcing, typing and certain accounting functions
- Updating and enhancing the client records we hold
- Analysis to help us manage our Company
- Legal and regulatory compliance
- The Financial Conduct Authority – who may visit our office in order to assess our compliance with the Rules and Regulations that are applicable for the services that we provide. We are under a duty to co-operate with our Regulator to the fullest extent. As part of these visits the Regulatory body may require access to your files and all the records we hold about you.
- Accounting Procedures - We are obliged to provide our regulatory body with confirmation from an independent accountant that our accounting practices accord with regulatory requirements. This involves our external accountants visiting our office to review our accounts files and procedures.
- Any such third parties accessing your files for these purposes themselves are under a duty to keep all information about you confidential. Please do not hesitate to contact us should you have any questions or objections to this.
- We do not copy such information to anyone outside the European Economic Area. All such third parties are required to maintain confidentiality in relation to your files.
- Training. We sometimes draw on client data to give compliance, best practice and regulatory guidance to our staff.

Your creditors may ask to visit our office in order to inspect and monitor the information, payment, processing and account status relating to your file given that they have a financial interest.

We are obliged to provide our regulatory body with confirmation from an independent accountant that our accounting practices accord with regulatory requirements. This involves our external accountants visiting our office to review our accounts files and procedures.

Our Regulator conducts visits to our office in order to assess our compliance with the Rules and Regulations that are applicable for the services that we provide. We are under a duty to co-operate with our Regulator to the fullest extent. As part of these visits the Regulatory body may require access to your files and all the records we hold about you.

We do not copy such information to anyone outside the European Economic Area. All third parties that we send or disclose your personal information to are required to maintain confidentiality in relation to your files.

3. Data Protection in respect of Money Laundering checks

We will ask you for personal data for the purposes of our money laundering checks, including a copy of your current passport or photographic driving licence. Such documentation will be processed only for the purposes of preventing money laundering and terrorist financing, or as otherwise permitted by law or with your express consent.

You consent to us retaining all such data we hold for you for six years. This is 12 months longer than the five year statutory period that we are duty bound to retain this information for.

If you do not agree to us doing so please contact us immediately.

Other than as set out above we will only disclose your personal information to the extent required for us to deliver our service to you by law, Court Order or as requested by other Government or law enforcement authority or our Regulatory body.

4. Our Obligations

As we hold/will hold information about you this gives rise to obligations under the General Data Protection Regulation (GDPR).

You have rights in relation to the information we hold about you. That includes the right to be informed what we hold, the right to have errors corrected and the right to have data deleted if we have no justification for holding it.

If we become aware of breaches of security with confidential information we have a duty to report breaches of security to you, our Regulator the Financial Conduct Authority and to the Information Commissioner's Office.

We may be legally liable in various ways if we fail to hold your data appropriately in accordance with the regulatory rules by which we are bound. The following is a summary of our obligations under data protection law, which we would be grateful if you could read carefully.

The Data Protection Principles: In processing your personal data we must be able to demonstrate that we comply with the "data protection principles". In brief these require us to ensure that your personal data is:

- processed lawfully, fairly and in a transparent manner
- collected for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes
- adequate, relevant and limited to what is necessary
- accurate and kept up to date
- kept for no longer than is necessary

- kept with appropriate security.

5. Grounds for Processing Personal Data:

We will only process your personal data if we have a legitimate justification for doing so.

We will usually process your personal data on the basis of your consent.

There are also circumstances where we may be entitled to process your data without consent. For example

- a. It is necessary for the performance of the contract for our services to which you have subscribed.
- b. It is necessary for compliance with any legal obligations we have.
- c. Or if it is necessary to protect your vital interests.

If you provide us with information about third parties, who may be unaware and they have not consented to us holding information about them. We will:

- Not record information about people unless we need to do so.
- Keep it secure.
- Delete it promptly when it is no longer needed by us.

6. Sensitive Personal Data

Sensitive personal data (referred to in the GDPR as “special categories of personal data”) can only be processed under strict conditions. Sensitive personal data includes information about your racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health or sex life and sexual orientation and physical or mental disability.

The usual grounds which entitle us to process such sensitive data are the following.

- a. Your explicit consent to us doing so. This includes your consent to us recording such information on our systems and disclosure to your creditors.
- b. It is necessary to protect your interests if you are physically or legally incapable of giving consent
- c. Data manifestly made public by you.
- d. It is necessary for the establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity.

Any sensitive data you supply to us will only be entered on our computer systems if you expressly agree to us doing so and if it’s necessary for the management of your IVA. We will only disclose such data to your creditors with your express approval also. Any

information which you agree to us entering on our systems is password protected and will be reviewed regularly to ensure that it is up to date.

In relation to mental health conditions which impact your ability to manage your financial affairs it is possible for you to voluntarily add information about any mental health condition on their credit files held by credit reference agencies. These are known as “notice of corrections”. This gives creditors prior notice of any mental health condition which can only be accessed by creditors once a credit search is made when a consumer is seeking access to credit. If you were to take such a step and make an entry on your credit file it would be your responsibility to update such a notice. The credit reference agencies have agreed a standard form of wording for the purposes of such notices. If and when such a notice is removed from your record it will not leave a trail/footprint on your credit file. Additionally it is possible to register vulnerabilities with the Vulnerable Registration Service (VRS). The VRS has been developed to assist vulnerable people protect themselves against the financial, social and personal hardship suffered as a result of debt and financial problems. It works so as to prevent inappropriate marketing and/or financial offers. It enables organisations with access to the register to identify potentially vulnerable circumstances and assist them in deciding on any customer engagement strategies from marketing, account management and arrears and collections. If we believe this to be of benefit to you we will let you know.

If you give us information about yourself we will record that information and use it for the purposes of delivering our services to you.

7. Sending personal data to others:

We will often need to share your personal data and confidential information with others such as creditors, Collection agencies or Solicitors that have been appointed by them and the Courts if legal action has been commenced. Before doing so we will consider these issues.

- Whether the organisation that we are proposing to send the information to really needs it?
- We will redact documents so that they do not include irrelevant and unnecessary confidential information where it is appropriate for us to do so
- We will also consider if we can rely on the recipient to keep the information secure. Most if not all of your creditors will be banking institutions that are bound by the same Data Protection rules and principles.

8. Keeping your Data secure

- We keep confidential papers in alarmed and locked offices when they are not in use.
- We have stringent procedures in place if it is necessary to take your information out of this office. All our laptops are encrypted for added security.

- We ensure that any confidential papers are shredded on disposal.

9. Keeping our IT systems secure

- At the outset of your instructions we will ask you for an email address should it be necessary to contact you urgently or is this is your preferred method of communication. Should you change your email address it is important that you contact us to let us know. This is important as if we receive an email from an unknown source we may not be able to open any attachments or links which may risk viruses being downloaded on our systems.
- We will ensure that the security and anti-virus software on our computers is updated frequently and any security weaknesses will be addressed immediately.
- Our computer hard drives, data sticks, floppy disks, CD-ROMs etc are physically destroyed when no longer required in accordance with our legal obligations.
- Electronic Equipment is destroyed using kill disc and individual folders will be permanently deleted from the system. Once deleted from the system electronic records are not recoverable even using forensic data recovery techniques.

10. Accounting Facility

The Company has policies in place to protect itself from the risk of funds being diverted.

The policies and procedures we have in place serve to protect against criminals seeking to divert funds.

We will ensure before dealing with any enquiry to:

- Check your identity. We will ask you to go through various security questions before sharing any information with you.
- We may ask you to put any request for information in writing if we are not sure about your identity and such cannot be immediately checked.

11. The storage of letters and statements that we receive from you and your creditors.

The responsibility for storage of files falls to the Data Protection Officer who must ensure that adequate and appropriate safeguards are in place for the rights and freedoms of our customers and clients. The Data Protection Officer has responsibility to ensure that data is destroyed securely..

The salient information contained in any correspondence we receive about your accounts from you and your creditors is entered onto our computer systems. Thereafter the correspondence

will be retained securely at our premises in a designated file we hold for you until such a time as your IVA is approved by your creditors or your contact with us terminates. Once your IVA is approved we will forward the entirety of the paper file we hold for you to the Supervisor of your Voluntary Arrangement.

If your contract with us terminates we will place your file in secure storage for a period of 6 years following the termination of your instructions. We are duty bound not to hold information any longer than is necessary. We will retain records for 6 years following the termination or conclusion of your IVA as this is when the statutory limitation period for any civil claims that may arise from our delivering our service to you expires. After this period we will destroy the paperwork securely in line with data protection guidelines.

You consent to us retaining such data for longer than the five year statutory period, unless you tell us otherwise. Data is retained for six years as data may be needed for the Company to provide compliance with any legal requirements or records may be needed in the event of litigation.

12. IVA's based on joint circumstances.

At the outset of your instructions to us if you are in a relationship and living with your partner and you both have outstanding debts, we will advise whether an IVA based on your joint circumstances is in your best interests, we will assume that we have your permission to act on the instructions of your partner. We will of course endeavour to discuss important issues with both of you both individually. However in circumstances where we experience difficulty in so doing that advice and information will be provided in writing to both of you initially, inviting you both to contact us in order that we can discuss matters further. If, however, we are unable to discuss the matter with both of you as stated above, we will assume we can act on the instructions of one of you. Of course an IVA is individual to you both. If you are not happy about this it is important that you contact us urgently.

13. Your Rights

- You have the following rights:
- A right to be informed as to what information we hold
- A right to access a copy of the information we hold
- A right to object or restrict our processing of your data if it is causing distress
- A right to prevent processing for direct marketing
- A right to have inaccurate personal data rectified, blocked, erased or destroyed
- A claim to compensation for damage caused by a breach of the Act
- You can request that all your personal data is removed from our Data base or you can request that personal data can be transferred to another system at no cost to you.
- To have data deleted if we have no justification for holding it.
- The right to lodge a complaint with the Information Commissioner's Office.

Any request for information as detailed above will be treated as a Subject Access Request and must be made in writing. We will do our utmost to respond to any such request within 30

days. In complex cases we may extend this period of compliance by up to a further 2 months. If this proves necessary we will let you know within the initial 30 day period and explain why an extension is necessary. We reserve the right to charge you for any unreasonable requests which we deem in our absolute discretion to be disproportionate, excessive or unfounded. Such fees will be proportionate to the administrative cost of providing the information. We will engage with you to come to a mutually beneficial outcome. Information will be provided in a secure format. If your personal data has been deleted we will inform you that this is the case.

14. Nuisance/Unwanted Telephone Calls

If you believe that you have been directly affected by our processing of your personal data you may contact the Information Commissioner's Office.

Following the General Data Protection Regulation 2018 coming into force, companies are now required to have your specific consent for making marketing calls. Consequently if you receive unsolicited telephone calls and you are happy about doing so this is something that you can report to the Information Commissioner's Office on 0303 1231113.

15. Consent to Receive Information

Quite apart from managing the preparation of your IVA we like to send present and past clients information that may be of interest to them. This includes information about legal developments changes in creditor policies or details about us and our services. If you consent to receiving such information please tick the box at the bottom of the Acknowledgement Form. Should you subsequently change your mind you can go to our website at www.moneysolve.co.uk/opt-out where you will be able to withdraw your previous consent to receive such communications or alternatively you could telephone us to let us know.

16. Data Protection Officer

The Company's Data Protection Officer Mike Davies has overall responsibility for data protection and this policy. If you have concerns about any of the matters referred to in this booklet please speak to Mr Davies.

Should you have any queries in relation to this booklet and how we process your data please don't hesitate to ask us.