UniLink Finance Ltd

Data Protection Policy and Operating Procedure

Next review date: 19/4/21

Why this policy exists

This data protection policy ensures that we:

- Comply with data protection law and follows good practice
- Protect the rights of staff, customers and partners
- Are open about how it stores and processes individuals' data
- Protect ourselves from the risks of a data breach

1. UniLink Finance needs to gather and use certain information about individuals. These can include customers, suppliers, business contacts, employees and other people the organisation has a relationship with or may need to contact wish to ensure that we conform at all times with both the letter and the spirit of the Data Protection Act 1998 ("DPA") and the GDPR. Furthermore, we expect all of our representatives to do the same.

2. In particular, we wish to ensure that we do not process "personal data" (as defined in the GDPR) without the consent of the relevant individual. We will obtain all necessary consent from any relevant individual before his/her personal information is passed.

3. Such consent will, for example, need to be obtained from:

    3.1 any individual or regulated body that we may be introducing a finance agreement to;

    3.2 all partners in a partnership;

    3.3 individual directors of limited liability companies where the tangible net worth is £50,000 or less; and

    3.4 any individual who will be providing a personal guarantee

4. Such consent will need to be expressed to:

    4.1 extend to all activities detailed in the Data Protection Consent, as amended by us from time to time in order to reflect GDPR best practice; and

    4.2 be effective whether or not we enter introduce a Finance Agreement with the customer as a result of the Proposal to which the consent applies.

    4.3 include our contact details should a customer wish to know which credit reference and/or fraud prevention agency has been used.

5. Furthermore, this consent will need to cover the following activities:

    5.1 allow us to share all personal information regarding an individual (including information obtained from other sources) for us/them to use that information for the purposes of research

and analysis, customer services or to contact the individual about other products/services, such contact to be by any means including email, telephone or post.

5.2 allow us to use all such personal information for credit assessment as part of the finance application, including carrying out credit reference agency searches and/or recording details with fraud prevention agencies; it must be clear to the individual that these searches/records will be available for others to access and use for purposes such as checking other finance applications, recovering debt, checking insurance proposals/claims and in connection with job applications/employment.

6. Confirmation that consent to search has been obtained in compliance with the terms of this Policy must be listed on each introduced finance application where required.

7. If the circumstances of a given transaction make it difficult for us to obtain such consent direct from any individual (for example, where finance is being arranged by one director/partner and you have no direct contact with his co-directors/partners), express confirmation must be obtained from the individual with whom you are dealing that he/she is authorised to give DPA consent on behalf of any other relevant individuals.

8. If requested we must inform the individual as to what their rights are under GDPR. Below is a list of such rights we will inform them of:

- To access their own personal data;
- To correct personal data;
- Erase personal data;
- Restrict data processing;
- Object to data processing (for example for marketing purposes);
- Receive the transfer of their personal data to another data controller (known as data portability).
- Not be subject to automated decision-making;
- Be notified of a data security breach within 1 month of such breach.

9. Personal Data Storage

All records will be capable of being reproduced in the English language on paper and be held for as long as is relevant for the purposes for which they are made in order that the following conditions are met:

1) the FCA and ICO must be able to access them readily and to reconstitute each key stage of the processing of each transaction;
2) it must be possible for any corrections or other amendments, and the contents of the records prior to such corrections and amendments, to be easily ascertained;
3) it must not be possible for the records otherwise to be manipulated or altered.

Personal Date records via email (signed consent forms) are stored within our secure 365 server and on each individual staff members PC secured by password. Paper records are stored in client files and archived and retained off site for the appropriate period.

10. Policy scope
This policy applies to (as appropriate):

All staff and volunteers
All contractors, suppliers and other people working on our behalf

It applies to all data that we hold relating to identifiable individuals, even if that information does not, in itself, identify an individual. This can include:
Names of individuals
Postal addresses
Email addresses
Telephone numbers
Location data
Online identifiers
Mobile data

11. Data use

When personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft:

- When working with personal data, employees should ensure the screens of their computers are always locked when left unattended.
- Personal data should never be transferred outside of the European Economic Area.
- Employees should not save copies of personal data to their own computers.
- Always access and update the central copy of any data.

12. Data accuracy

The law requires us to take reasonable steps to ensure data is kept accurate and up to date.
The more important it is that the personal data is accurate, the greater the effort we should put into ensuring its accuracy.

It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be held in as few places as necessary. Staff should not create any unnecessary additional data sets.
- Staff should take every opportunity to ensure data is updated. For instance, by confirming a customer's details when they call.
- We will make it easy for data subjects to update the information we hold about them.
- Data should be updated as inaccuracies are discovered. For instance, if a customer can no longer be reached on their stored telephone number, it should be removed from the database.

General staff guidelines

- The only people able to access data covered by this policy should be those who need it for their work.
- Data should not be shared informally. When access to confidential information is required, employees can request it from their line managers.
- We will provide training to all employees to help them understand their responsibilities when handling data.
- Employees should keep all data secure, by taking sensible precautions and following the guidelines below.
- In particular, strong passwords must be used and they should never be shared.
- Personal data should not be disclosed to unauthorised people, either within the company or externally.
- Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of.

- Employees should request help from their line manager or the data protection officer if they are unsure about any aspect of data protection.