Privacy Statement: Contractors

Unless otherwise stated, Unity Trust Bank is the data controller for the information you provide during the engagement process and any subsequent period of contract work undertaken within the bank. If you have any queries about the process or how we handle your information please contact us at hr@unity.co.uk.

1. **What will we do with the information you provide to us?**

The information you provide during the engagement/contract process will be used for assessing your suitability and if successful in providing services to the bank, to enable the bank to fulfill the performance of the contract of engagement or to fulfil legal or regulatory requirements if necessary.

We will not share any of the information you provide during the process with any third parties for marketing purposes, or store any of your information outside of the European Economic Area. The information you provide will be held securely by us and/or our data processors whether the information is in electronic or physical format.

2. **What information do we ask for, and why?**

We will only process your personal information for the purpose for which we collect it and we will not retain it for longer than necessary.

The information we ask for is used to assess your suitability for engagement. You don't have to provide what we ask for but it might affect your ability to be considered in providing services to the Bank if you don't.

If we need to use your information for an unrelated purpose we will contact you and we will explain the legal basis that allows us to do so. Please note that we may process your personal information without your knowledge or consent, in compliance with our obligations in the case of criminal investigation.

If you are applying directly to the bank or via a third party, we will receive a copy of your CV as part of the contract process. This will be stored within the HR team whilst the process is ongoing.

If you apply via a third party, the CV will be received and processed as per your agreement with them.

Service Agreement

If we agree to engage your services we will ask you for information so that we can carry out background screening checks. This includes contact details, previous contracts and employment gaps, education and for answers to questions relevant to the services you will be providing us with. Only our HR team will have access to this information.

All background screening checks must be passed successfully or we may withdraw the offer or terminate your engagement with us.

We are required to confirm the identity of our contractors, their right to work in the United Kingdom and to seek assurance as to their trustworthiness, integrity and reliability. *Please note: if you engage with the bank in a Senior Manager or Certification role, there are several checks which will be repeated during your tenure with the bank, these are marked below with - **

You will therefore be required to provide:

- Proof of your identity and confirmation of right to work in the UK – you will be asked to attend our office with original documents in advance of your start date, we will take copies.

- Proof of your qualifications – you will be asked to attend our office with original documents, we will take copies*
- You will be asked to complete a declaration disclosing issues relating to your financial solvency and adverse credit history, court judgments, previous directorships and company filing history. You will also be asked to declare any unspent criminal convictions*
- You will also be asked to complete a Basic or Standard Criminal Record check via the Disclosure and Barring Service which will verify your declaration of unspent convictions (and spent convictions where a standard check is required). The HR team will receive the results and destroy the certificate immediately. The certificate number, date and result will be held to evidence satisfactory result*
- We will also carry out credit and fraud checks using a data processor* . For more information on how we work with Cifas please see Annex 1 at the end of this document or you can refer to: https://www.cifas.org.uk/fpn..
- Results of these checks will be seen by the HR team only and retained during your engagement and for 12 months after your contract ends. If the agreement is subsequently withdrawn after these checks have been completed, the data will remain on file for 6 months.

The data collected will be held and stored for the duration of your engagement with the bank and six years after your engagement has ended.

3. How do we make decisions about who we engage with?

Final decisions are made by the manager of the area requiring the services and members of our HR team. All information gathered during the process is considered.

4. What data is collected after I have started with Unity Trust Bank?

Once you have started with us we will also ask for Emergency contact details – so we know who to contact in case you have an emergency whilst on site at Unity.

If you are providing services directly to the bank you will also be required to provide your company bank details. This information will only be used for the duration of your engagement and then erased.

5. Use of data processors

During your engagement, there may be other occasions when we are collecting or using data to fulfil the performance of the contract and associated benefits either directly within the Bank or via a data processor.

Data processors are third parties who provide elements of our contract and other human resource management services relevant to your engagement. We have contracts in place with our data processors and only use processors who provide sufficient guarantees to implement appropriate technical and organisational measures which ensure that processing will meet the requirements of the General Data Protection Regulation and protect your rights as a data subject. This means that they cannot do anything with your personal information unless we have instructed them to do it.

They will not share your personal information with any organisation apart from us. They will hold it securely and retain it for the period we instruct.

Contract/Search Agencies

If you engage via an agency, they will be the Data Controller for the documents you provide to them and they subsequently forward to us e.g. CV. Please contact the relevant agency and ask to see their privacy notice if you require more information.

Skillserve

To ensure you can complete all mandatory training, we will also supply our online training provider, Skillserve provided by Unicorn Training with your first name, surname and unity email address.

Here is a link to their Privacy Notice.

https://www.unicorntraining.com/privacy-and-cookie-policy

6. Other Data Processors

On occasion the bank may also carry out surveys using external providers. The bank may provide unity email addresses to suppliers to enable them to facilitate these surveys with impartiality.

7. Your right to withdraw consent

You have the right to withdraw your consent to the collection, processing and transfer of your personal information for specific processing at any time., Once we have received notification that you have withdrawn your consent, we will no longer process your information unless we have another legitimate basis to do so in law and/or it is required for the necessary performance of the contract. This will not affect the lawfulness of processing based on consent before its withdrawal.

8. How long do we keep your information for?

If you are successful in providing services to the bank, the information you provide during the process will be retained by us as part of your contractor file for the duration of your engagement, plus 1 year following the end of your engagement. This includes your criminal records declaration, credit, fraud, and qualifications.

If you are unsuccessful at any stage of the process, the information you have provided or we have gathered (such as interview notes or background check results) until that point will be retained for 6 months.

9. What are your rights?

At Unity Trust Bank we recognise that your data is important to you and therefore we are committed to supporting you with your data protection rights. These include:

- (where we rely on your consent to process your personal information) the right to withdraw consent to the processing of your personal information,
- the right to request access to your personal information (a “data subject access request”);
- to correct any mistakes on our records;
- to erase or restrict your personal information where it is no longer needed for the purpose for which they were obtained or used;
- the right to object to our use of your personal information based on legitimate business interests, including for profiling and marketing; and
- the right, in certain circumstances, to receive a machine-readable copy of, the personal information you provided to us.

You will not have to pay a fee to access your personal data (or to exercise any of the other rights). However, we may charge a reasonable fee if your request is clearly unfounded, repetitive or excessive. We will handle any request to exercise your rights in accordance with applicable law.

If you wish to exercise any of these rights please write to us at: hr@unity.co.uk or

PO BOX 7207 – HR only
Planetary Road
Willenhall
WV1 9DN

Please ensure you include the subject line 'Personal information request' and supply the following details:

- First name(s) & surname
- Address & postcode
- Details of the type of information you are seeking
- Proof of Identity – this needs to be a document containing a photograph and signature such as a driving license.

In your request, please make clear what right you would like to exercise. Providing us with this information will help us to quickly identify and deal with your request.

Please also specify the format you require the information in and be specific about the data you would like to see or have altered/deleted. If this is unclear we will contact you to discuss your request.

10. What should you do if you wish to make a complaint or raise a query about the way your data is being processed?

Unity Trust Bank aims to meet the highest standards when collecting and using personal information. For this reason, we take any complaints we receive about this very seriously. We encourage people to bring it to our attention if they think that our collection or use of information is unfair, misleading or inappropriate. We would also welcome any suggestions for improving our procedures.

If you wish to make a complaint about the way we have processed your personal information, you can contact the Data Protection Manager at Unity Trust Bank providing details of your complaint and your full name and contact details. If you are unhappy with the response received or wish to seek further guidance, you can also raise your concerns with the statutory body which oversees data protection law, Information Commissioners Office – www.ico.org.uk/concerns.

11. Changes to our Privacy Statement

We regularly review our Privacy Statement and will publish any updates on our webpage. This Privacy Statement was last updated on the date as set out at the top of this Privacy Statement.

12. Contacting us?

If you have any questions, or feedback about this Privacy Statement, please get in touch with our Data Protection Manager:

Email: us@unity.co.uk

Call: 0345 140 1000

Write to us at: Unity Trust Bank, PO Box 7193, Planetary Road, Willenhall, WV1 9DG

Annex 1: CIFAS FAIR PROCESSING NOTICE

1. We will check your details against the Cifas databases established for the purpose of allowing organisations to record and share data on their fraud cases, other unlawful or dishonest conduct, malpractice, and other seriously improper conduct ("Relevant Conduct") carried out by their staff and potential staff. "Staff" means an individual engaged as an employee, director, trainee, homeworker, consultant, contractor, temporary or agency worker, or self-employed individual, whether full or part time or for a fixed-term.

2. The personal data you have provided, we have collected from you, or we have received from third parties will be used to prevent fraud and other relevant conduct and to verify your identity.

3. Details of the personal information that will be processed include: name, address, date of birth, any maiden or previous name, contact details, document references, National Insurance Number, and nationality. Where relevant, other data including employment details will also be processed.

4. We and Cifas may also enable law enforcement agencies to access and use your personal data to detect, investigate, and prevent crime.

5. We process your personal data on the basis that we have a legitimate interest in preventing fraud and other Relevant Conduct, and to verify identity, in order to protect our business and customers and to comply with laws that apply to us. This processing of your personal data is also a requirement of your engagement with us.

6. Cifas will hold your personal data for up to six years if you are considered to pose a fraud or Relevant Conduct risk.

CONSEQUENCES OF PROCESSING

7. Should our investigations identify fraud or any other Relevant Conduct by you when applying for or during the course of your engagement with us, your new engagement may be refused or your existing engagement may be terminated or other disciplinary action taken (subject to your rights under your existing contract and under employment law generally).

8. A record of any fraudulent or other Relevant Conduct by you will be retained by Cifas and may result in others refusing to employ you. If you have any questions about this, please contact us using the details provided.

DATA TRANSFERS

9. Should Cifas decide to transfer your personal data outside of the European Economic Area, they will impose contractual obligations on the recipients of that data to protect your personal data to the standard required in the European Economic Area. They may also require the recipient to subscribe to 'international frameworks' intended to enable secure data sharing.

YOUR RIGHTS

10. Your personal data is protected by legal rights, which include your rights to object to our processing of your personal data, request that your personal data is erased or corrected, and request access to your personal data.

11. For more information or to exercise your data protection rights, please contact us using the contact details provided.

12. You also have a right to complain to the Information Commissioner's Office which regulates the processing of personal data.