

# DATA PROTECTION NOTICE FOR EMPLOYEES

## 1. Introduction

This notice explains what personal data we hold about you, how we collect it, and how we use and may share such information about you during your employment and after it ends ("Personal Data"). We are required to notify you of this Personal Data under applicable data protection legislation. Personal Data means any information about an individual from which that person can be identified. It does not include data where the person's identity has been removed (anonymous data).

Please ensure that you read this notice and any other similar notices we may provide to you from time to time when we collect or process personal data about you.

Where it is necessary for us to collect and processes any criminal conviction or offence data a copy of our Criminal Records Information Notice will be made available

For the purposes of this notice, the controller of your Personal Data is Pepper Money (PMB) Limited of registered office address 4 Capital Quarter, Tyndall Street, Cardiff, Wales, CF10 4BZ ("**Pepper Money**", "**the Company**", "**we**" or "**us**"). This means that we are responsible for deciding how we hold and use Personal Data about you.

Pepper Money as a 'data controller', gathers and uses certain Personal Data about you for the purposes of your employment with Pepper Money.

Pepper Money belongs to the Pepper Money UK Group and the global Pepper group of companies "Pepper Group Entities" a group of different legal entities located around the world. You can find more details about the Pepper Group here: <https://www.pepper.money/about-us>.

## 2. Data Protection Principles

We will comply with data protection law. This says that the Personal Data we hold about you must be:

1. Used lawfully, fairly and in a transparent way.
2. Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes.
3. Relevant to the purposes we have told you about and limited only to those purposes.
4. Accurate and kept up to date.
5. Kept only as long as necessary for the purposes we have told you about.
6. Kept securely.

## 3. Scope

This notice applies to every employee of the Company (including temporary or fixed term contract employees, ex-employees and secondees) and classes of workers such as consultants, representatives, former applicants, agency, casual workers, contractors, contract workers and those on work placements.

## 4. The kind of information we hold about you

We may collect, store, and use the following categories of Personal Data about you:

- **Contact details** including title, name, address, home and mobile phone numbers, email address;
- **Recruitment information** collected during the recruitment process that we retain during your employment – see Data Protection Privacy Notice (Recruitment), available on the Pepper Money website and HR comms hub;
- **Employment records** including employment contract information, job title, 1-2-1 records, performance management records including probation records, details of your time and attendance records including personal schedule and office attendance, absence management meetings, appraisals and performance reviews, details of your probation/performance/performance management/counselling notes/ development/improvement plans (if any), details of call monitoring and/or Training & Competence records, including test and exam results;
- **Bank account details, payroll records and tax status information;**
- **National Insurance number;**
- **Date of birth;**
- **Details of leave arrangements** including in relation to maternity, paternity, adoption, shared parental, bereavement and other types of leave or payments, as outlined in our Family Friendly Policy, available on the HR comms hub;
- **Marital status and dependents;**
- **Next-of-kin and emergency contacts;**
- **Your nationality and immigration status;**
- **Salary, annual leave, pension and benefits information;**
- Where relevant, **details of your share and/or other incentive arrangements**, and all information included in these and necessary to implement and administer them;
- **Information relating to regular credit and/or fraud checks** (see Appendix 1);
- **Disciplinary and grievance information;**
- **Details of qualifications and certificates** e.g. CeMap, first aid, fire marshal;
- **Photographs;**
- **CCTV footage and other information obtained through electronic means** such as swipe card or desk booking application records;
- **Information about your use of our systems** including IT, communication and other systems, and other monitoring information;
- **Details of your use of business-related social media**, such as LinkedIn;
- **Your use of public social media** (only in very limited circumstances), to check specific risks for specific functions within our organisation; you will be notified separately if this is to occur);
- **Information contained in any resignation letter, exit interview form;**
- **Information and opinions expressed in surveys; and**
- **Your signature.**

We may also collect certain special categories of Personal Data:

- **Your racial or ethnic origin, gender and sexual orientation, religious or similar beliefs, social economic background;**
- **Health information** including information in your sickness and absence records (including special categories of Personal Data regarding your physical and/or mental health, fit notes, Return to Work forms, occupational health assessments, employment support assessments, information about your health disclosed in medical questionnaire and/or risk assessments;
- **Criminal records information**, including the results of Disclosure and Barring Service (DBS) checks (refer to Criminal Records Information Privacy Notice); and/or
- **Details relating to your Fitness & Propriety** in relation to the FCA's Senior Managers and Certification Regime (SMCR) and/or conduct rules.

Certain of the categories above may not apply to you if you are an agency worker, independent contractor, freelancer, volunteer, intern, on student placement or on work experience placement.

## 5. How we collect the information

We may collect Personal Information from you, your personnel records, recruitment providers and agencies, the Home Office, share scheme administrators, pension administrators or trustees, your doctors, from medical and occupational health professionals, employment support programmes, we engage and from our insurance benefit administrators, benefits portal provider, talent assessment platforms, relevant professional bodies, the Disclosure and Barring Service (DBS), credit search agencies, background check provider (including but not limited to People Check), the relevant fraud sharing database (see Appendix 1), the Department of Work & Pensions, other employees, consultants and other professionals that we may engage (e.g. to advise us generally and/or in relation to any grievance, conduct appraisal or performance/absence review procedure), systems administration including door entry system, CCTV, computer activity logs, internet browsing history, firewall logs, internet proxy logs, application logs, remote access logs, email and instant messaging platforms, telephone system, voicemail, company mobile phone records, or any other company asset issued to you as part of your role.

We will collect additional personal information in the course of job-related activities throughout the period of you working for us.

## 6. Why we collect the information and how we use it

We will only use your Personal Data when the law allows us to. We will typically collect and use Personal Data for the following purposes:

- for the performance of a contract with you, or to take steps to enter into a contract; (including with the wider Pepper Group)
- for compliance with a legal or regulatory obligations (e.g. our obligations to you as your employer under employment protection and health safety legislation, and under statutory codes of practice, such as those issued by the Advisory, Conciliation and Arbitration Service or to fulfil the firms obligations as a regulated firm);
- for the purposes of our legitimate interests or those of a third-party (such as a benefits provider), but only if these are not overridden by your interests, rights or freedoms.

We may also use your Personal Data in the following situations, which are likely to be rare:

- Where we need to protect your interests (or someone else's interests), for example, in an emergency.
- Where it is needed in the public interest or for official purposes.

## 7. Situations in which we will use your Personal Data

We need all the categories of information in the list above primarily to allow us to perform our contract with you and to enable us to comply with legal and/or regulatory obligations. In some cases, we may use your Personal Data to pursue legitimate interests, provided your interests and fundamental rights do not override those interests. The situations in which we will process your Personal Data are listed below. We have indicated the purpose or purposes for which we are processing or will process your Personal Data, as well as providing a description of which categories of data are involved (identified in **bold** in the above list). Where a legitimate interest is involved, we state what the legitimate interest is

Activity	Category of data	Purpose(s)
Administering the contract we have entered into with you	<ul style="list-style-type: none"> <li>• Contact details;</li> <li>• Recruitment information;</li> <li>• Employment records;</li> <li>• Your signature.</li> </ul>	<ul style="list-style-type: none"> <li>• Performance of a contract with you; and</li> <li>• Complying with legal/regulatory obligations.</li> </ul>
Paying you (inclusive of approved expenses) and, if you are an employee or deemed employee for tax purposes, deducting tax and National Insurance contributions (NICs)	<ul style="list-style-type: none"> <li>• Contact details</li> <li>• Gender</li> <li>• Bank account details, payroll records and tax status information;</li> <li>• National Insurance number; and/or</li> <li>• Salary, annual leave, other types of leave (e.g. paternity/maternity), pension and benefits information.</li> </ul>	<ul style="list-style-type: none"> <li>• Performance of a contract with you; and</li> <li>• Complying with legal/regulatory obligations.</li> </ul>
Providing Company approved benefits to you (including but not limited to) pension, life assurance benefits	<ul style="list-style-type: none"> <li>• Contact details;</li> <li>• Bank account details, payroll records and tax status information;</li> <li>• Employment records;</li> <li>• Marital status and dependents;</li> <li>• Next of kin and emergency contacts;</li> <li>• Date of birth.</li> </ul>	<ul style="list-style-type: none"> <li>• Performance of a contract with you; and</li> <li>• Complying with legal/regulatory obligations.</li> </ul>
Enrolling you in a pension arrangement in accordance with our statutory automatic enrolment duties	<ul style="list-style-type: none"> <li>• Contact details;</li> <li>• Gender</li> <li>• Bank account details, payroll records and tax status information;</li> <li>• Date of birth</li> <li>• Pension information</li> </ul>	<ul style="list-style-type: none"> <li>• Complying with legal/regulatory obligations.</li> </ul>

Activity	Category of data	Purpose(s)
Liaising with the trustees or managers of a pension arrangement operated by a group company, your pension provider, benefits broker and any other provider of employee benefits	<ul style="list-style-type: none"> <li>• Contact details;</li> <li>• Bank account details, payroll records and tax status information;</li> <li>• Marital status and dependents;</li> <li>• Next of kin and emergency contacts.</li> </ul>	<ul style="list-style-type: none"> <li>• Complying with legal/regulatory obligations.</li> </ul>
Business management and planning, including accounting and auditing	<ul style="list-style-type: none"> <li>• Employment records;</li> <li>• Bank account details, payroll records and tax status information;</li> <li>• Details of leave arrangements;</li> <li>• Details of your share and/or other incentive arrangements;</li> <li>• Disciplinary and grievance information;</li> </ul>	Performance of a contract with you; <ul style="list-style-type: none"> <li>• <b>Legitimate interests</b> (managing our workforce and carrying out resource planning; manage usage &amp; security of our buildings; managing our workforce);</li> <li>• Complying with legal/regulatory obligations.</li> <li>• Fulfilment of Contractual terms and benefits (including discretionary benefits)</li> </ul>
Conducting performance reviews, managing performance, and determining performance requirements	<ul style="list-style-type: none"> <li>• Employment records;</li> <li>• Details of leave arrangements;</li> <li>• Disciplinary and grievance information.</li> <li>• Details relating to your fitness &amp; propriety.</li> </ul>	<ul style="list-style-type: none"> <li>• <b>Legitimate interest</b> (managing, retaining and developing our workforce)</li> </ul>
Making decisions about salary reviews and compensation	<ul style="list-style-type: none"> <li>• Employment records;</li> <li>• Details of leave arrangements;</li> <li>• Door Logs, Desk Booking application and HRIS profile (inclusive of name, day/time of arrival/departure)</li> </ul>	<ul style="list-style-type: none"> <li>• Performance of a contract with you;</li> <li>• <b>Legitimate interest</b> (to manage our workforce).</li> <li>• Fulfilment of Contractual terms and benefits (including discretionary benefits such as bonus payments)</li> <li>• Consent where relevant.</li> </ul>

Activity	Category of data	Purpose(s)
Assessing qualifications for a particular job or task, including decisions about promotions	<ul style="list-style-type: none"> <li>• Employment records;</li> <li>• Education records</li> </ul>	<ul style="list-style-type: none"> <li>• <b>Legitimate interests</b> (staff retention and development)</li> </ul>
Making decisions about your continued employment or engagement	<ul style="list-style-type: none"> <li>• Employment records;</li> <li>• Disciplinary and grievance information;</li> <li>• Health information;</li> <li>• Information about your use of our systems and applications;</li> <li>• Criminal records information;</li> <li>• CCTV footage and other information obtained through electronic means;</li> <li>• Details relating to your fitness &amp; propriety;</li> <li>• Your use of public social media.</li> </ul>	<ul style="list-style-type: none"> <li>• <b>Legitimate interests</b> (to manage our workforce).</li> </ul>
Making arrangements for the termination of our working relationship	<ul style="list-style-type: none"> <li>• Employment records;</li> <li>• Bank account details, payroll records and tax status information;</li> <li>• Details of leave arrangements;</li> <li>• Salary, annual leave, pension and benefits information.</li> </ul>	<ul style="list-style-type: none"> <li>• <b>Legitimate interest</b> (to manage our workforce).</li> </ul>
Education, training and development requirements	<ul style="list-style-type: none"> <li>• Employment records;</li> <li>• Details of qualifications and certificates;</li> <li>• Details relating to your fitness &amp; propriety.</li> </ul>	<ul style="list-style-type: none"> <li>• Performance of a contract with you;</li> <li>• <b>Legitimate interest</b> (to develop our workforce).</li> </ul>

Activity	Category of data	Purpose(s)
Dealing with legal disputes involving you, or other employees, workers and contractors, including accidents at work	<ul style="list-style-type: none"> <li>• Employment records;</li> <li>• Disciplinary and grievance information;</li> <li>• Health information;</li> <li>• Your signature;</li> <li>• Personal characteristics;</li> <li>• Details relating to your fitness &amp; propriety.</li> </ul>	<ul style="list-style-type: none"> <li>• <b>Legitimate interest</b> (to manage our workforce).</li> <li>• Complying with legal/regulatory obligations.</li> </ul>
Ascertaining your fitness to work	<ul style="list-style-type: none"> <li>• Details relating to your fitness &amp; propriety;</li> <li>• Health information;</li> <li>• Your signature.</li> </ul>	<ul style="list-style-type: none"> <li>• <b>Legitimate interest</b> (to manage our workforce).</li> <li>• Complying with legal/regulatory obligations.</li> <li>• Consent where relevant.</li> </ul>
Managing sickness absence	<ul style="list-style-type: none"> <li>• Employment records;</li> <li>• Salary, annual leave, pension and benefits information;</li> <li>• Details of leave arrangements;</li> <li>• Health information.</li> </ul>	<ul style="list-style-type: none"> <li>• <b>Legitimate interest</b> (to manage our workforce).</li> <li>• Complying with legal/regulatory obligations.</li> <li>• Consent where relevant.</li> </ul>
Complying with health and safety obligations	<ul style="list-style-type: none"> <li>• Employment records;</li> <li>• Health information;</li> <li>• Information and opinions expressed in surveys.</li> </ul>	<ul style="list-style-type: none"> <li>• To comply with legal/regulatory obligations.</li> <li>• Consent where relevant.</li> </ul>
To prevent fraud	<ul style="list-style-type: none"> <li>• Contact details;</li> <li>• Employment records;</li> <li>• Information about your use of our systems and applications;</li> <li>• IP Addresses;</li> <li>• Background and other relevant checks.</li> </ul>	<ul style="list-style-type: none"> <li>• To comply with legal/regulatory obligations;</li> <li>• Legitimate interests (to protect the reputation of our business).</li> </ul>

Activity	Category of data	Purpose(s)
To monitor your use of our information and communication systems to ensure compliance with our IT policies	<ul style="list-style-type: none"> <li>• CCTV footage and other information obtained through electronic means;</li> <li>• Information about your use of our systems and applications;</li> <li>• Information and opinions expressed in surveys.</li> </ul>	<ul style="list-style-type: none"> <li>• To comply with legal/regulatory obligations.</li> <li>• <b>Legitimate interests</b> (to protect the security and integrity of our information and communication systems).</li> </ul>
To ensure network and information security, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution	<ul style="list-style-type: none"> <li>• CCTV footage and other information obtained through electronic means;</li> <li>• Information about your use of our systems and applications.</li> </ul>	<ul style="list-style-type: none"> <li>• <b>Legitimate interests</b> (to protect the security and integrity of our information and communication systems).</li> </ul>
To conduct data analytics studies to review and better understand employee retention and attrition rates	<ul style="list-style-type: none"> <li>• Information contained in any resignation letter, exit interview form;</li> <li>• Information and opinions expressed in surveys.</li> <li>• Employee records.</li> </ul>	<ul style="list-style-type: none"> <li>• <b>Legitimate interest</b> (to manage and grow our workforce).</li> </ul>
Diversity monitoring	<ul style="list-style-type: none"> <li>• Your racial or ethnic origin, gender (including reassignment) and sexual orientation, disability, age, religious or similar beliefs;</li> <li>• Social economic background;</li> <li>• Health information;</li> <li>• Information and opinions expressed in surveys.</li> </ul>	<ul style="list-style-type: none"> <li>• <b>Legitimate interests</b> (to review diversity in business, managing, retaining and developing our workforce)</li> <li>• Substantial public interest (Equality of opportunity or treatment; Racial and ethnic diversity at senior levels)</li> </ul>



Activity	Category of data	Purpose(s)
To undertake external marketing activities and internal activities including establishing organisational charts and issuing newsletters, notices, and updates	<ul style="list-style-type: none"> <li>• Contact details (name and work email address, telephone, home address);</li> <li>• Details of your use of business-related social media;</li> <li>• Photographs;</li> <li>• Information and opinions expressed in surveys.</li> </ul>	<ul style="list-style-type: none"> <li>• <b>Legitimate interests</b> (to market our business); and</li> <li>• Consent where relevant.</li> </ul>
To issue building access passes	<ul style="list-style-type: none"> <li>• Photographs; and</li> <li>• Contact details (name).</li> </ul>	<ul style="list-style-type: none"> <li>• Legitimate interests (to manage security of our buildings).</li> <li>• Consent where relevant;</li> </ul>
To review and analyse data relating to monitoring of office utilisation	<ul style="list-style-type: none"> <li>• Door Logs, Desk Booking application and HRIS profile (inclusive of name, day/time of arrival/departure);</li> <li>• Geolocation Data;</li> <li>• Information about your use of our systems and applications;</li> <li>• IP Addresses;</li> <li>• Employment records;</li> <li>• Details of leave arrangements;</li> <li>• Health information.</li> </ul>	<ul style="list-style-type: none"> <li>• To comply with legal/regulatory obligations;</li> <li>• Legitimate interests (to manage usage &amp; security of our buildings; to manage our workforce);</li> <li>• Fulfilment of Contractual terms and benefits (including discretionary benefits);</li> <li>• Consent (where relevant).</li> </ul>

Activity	Category of data	Purpose(s)
To meet our obligations relating to legislative and regulatory reporting	<ul style="list-style-type: none"> <li>• Employment records;</li> <li>• Bank account details, payroll records and tax status information;</li> <li>• Details relating to your fitness &amp; propriety;</li> <li>• Health information;</li> <li>• Disciplinary and grievance information;</li> <li>• Your signature;</li> <li>• Personal characteristics;</li> </ul>	<ul style="list-style-type: none"> <li>• To comply with legal/regulatory obligations;</li> <li>• and/or Legitimate interests (to manage our workforce).</li> <li>• Consent where relevant.</li> </ul>

Some of the above grounds for processing will overlap and there may be several grounds which justify our use of your Personal Data.

### **If you fail to provide Personal Data**

If you fail to provide certain information when requested, we may not be able to perform the contract we have entered into with you (such as paying you or providing a benefit), or we may be prevented from complying with our legal/regulatory obligations (such as to ensure the health and safety of our workers).

### **Change of purpose**

We will only use your Personal Data for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use your Personal Data for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

Please note that we may process your Personal Data without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

## **8. Special categories of Personal Data**

We do not need your consent if we use special categories of Personal Data to carry out our legal/regulatory obligations or exercise specific rights related to employment law. We may ask for your written consent for us to process certain particularly sensitive Personal Data. In doing so, we will provide you with full details of our request to help you to make a decision. It is not a condition of your contract with us that you agree to any request for consent from us.

We do not need your consent where we process your Personal Data to protect you or another person from harm, to protect your well-being or if we reasonably believe that you need care and support, are at risk of harm and are unable to protect yourself.

### **How we use particularly special categories of Personal Data**

Some special categories of Personal Data require higher levels of protection. We need to have further justification for collecting, storing and using this type of Personal Data. We have an appropriate policy document and safeguards in place which we are required by law to maintain when processing such data. We may process special categories of personal information in the following circumstances:

1. In limited circumstances, with your explicit written consent.
2. Where we need to carry out our legal/regulatory obligations or exercise rights in connection with employment.
3. Where it is needed in the public interest, such as for equal opportunities monitoring or in relation to our occupational pension scheme.
4. Where it is necessary to protect you or another person from harm.

Less commonly, we may process this type of information where it is needed in relation to legal claims or where it is needed to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.

### **Situations in which we will use your special categories of Personal Data**

We will use information about your physical or mental health, or disability status, to:

- ensure your health and safety in the workplace;
- assess your fitness to work;
- provide appropriate workplace adjustments;
- monitor and manage sickness absence
- monitor and manage equality and diversity within the workforce; and
- administer benefits including statutory maternity pay, statutory sick pay, and pensions and permanent health insurance.

We need to process this information to exercise rights and perform obligations in connection with your employment.

- If we reasonably believe that you or another person are at risk of harm and the processing is necessary to protect you or them from physical, mental or emotional harm or to protect physical, mental or emotional well-being.
- We will use information about your race or nationality or ethnic origin, religious, philosophical or moral beliefs, your sexual life or sexual orientation, social economic background to ensure meaningful equal opportunity monitoring and reporting.

## **9. Information about Criminal Convictions**

We may only use information relating to criminal convictions where the law allows us to do so. This is usually where that processing is necessary to carry out our obligations and provided, we do so in line with our Data Privacy Notice.

We will only collect information about criminal convictions during your employment if it is appropriate given the nature of the role and where we are legally able to do so. Where appropriate, we will collect information about criminal convictions as part of the recruitment process or we may be notified of such information directly by you in the course of you working for us. We will use information about criminal convictions and offences to carry out criminal record checks for those carrying out roles that have access to personal customer and/or colleague data.

We may process such Personal Data where it is necessary for us to process your criminal record information for the purposes of preventing or detecting unlawful acts, to protect the public against dishonesty, or where it is necessary for the purposes of complying with a regulatory requirement or for the purposes of preventing fraud or a particular kind of fraud. We have in place an appropriate policy and safeguards which we are required by law to maintain when processing such data.

Further information about our processing of criminal conviction and offence data can be found in our Criminal Records Information Notice a copy of which can be obtained from our website or the Hub.

## 10. How we may share the information

We may also need to share some of the above categories of Personal Data with other parties, such as Pepper Group Entities, and our third-party service providers, IT system and network providers, our professional and legal providers, medical advisers and occupational health professionals, auditors and regulators, training providers, talent assessment providers, facilities providers, marketing providers (including gift providers), business continuity consultants, survey providers, recruitment/HR consultants, professional advisers, benefits and insurance providers, payroll administrators and trustees, graduate/internship programme providers, Welsh Assembly Government, Welsh European Funding Office, The European Social Fund, Cnect Wales (formerly known as Welsh Contact Centre Forum), credit search and fraud agencies (see Appendix 1), other Graduate Programme consortium members, other employers (e.g. in relation to Regulatory Reference obligations under the FCA's SMCR) and other relevant third parties such as the Inland Revenue or with potential purchasers, investment/funding partners (due diligence) of some or all of our business or on a re-structuring. Where possible, information will be anonymised.

We may need to share Personal Data for a number of reasons such as to fulfil obligations under our employment contract with you, provide suitable benefits, enable regular checks to be completed (e.g. Fit & Proper check, credit checks), to ensure compliance with company policies or for internal reporting purposes, or for other legitimate business purposes.

The recipient of the Personal Data will be bound by confidentiality obligations. We do not allow our third-party service providers to use your personal data for their own purposes. We only permit them to process your personal data for specified purposes and in accordance with our instructions. We may also be required to share some Personal Data with our regulators or as required to comply with the law.

## 11. Where information may be held

Information may be held securely at our offices or on our IT systems, third-party agencies, service providers, representatives and/or agents as described above.

## 12. How long we keep your information

We keep your information during and after your employment for no longer than is necessary for the purposes for which the Personal Data is processed. Further details on this are available on request from [DPO@pepper.money](mailto:DPO@pepper.money)

## 13. Is your Personal Data transferred outside the UK

We may sometimes transfer your personal data outside the UK to other Pepper Group Entities and other third-party recipients. If it is processed within Europe or other parts of the European Economic Area (EEA) then it is protected by data protection standards. Some countries outside the EEA do have adequate protection for Personal Data under laws that apply to us. We will make sure that suitable safeguards are in place before we transfer your Personal Data to countries outside the EEA which do not have adequate protection under laws that apply to us.

Where such transfers occur, we ensure that: a) they do not occur without our prior written authority; and b) such transfers of your personal data are subject to the Standard (Model) Contract Clauses, as permitted under applicable data protection legislation.

## 14. Your rights

It is important that the personal information we hold about you is accurate and current. Please keep us informed if your personal information changes during your working relationship with us.

Please contact Pepper Money's Data Protection Officer (DPO) at [DPO@pepper.money](mailto:DPO@pepper.money) if (in accordance with applicable law) you would like to correct or request access to information that we hold relating to you or if you have any questions about this notice. You also have the right to ask for some, but not all, of the information we hold and process to be erased (the 'right to be forgotten') in certain circumstances. Our Data Protection Officer will provide you with further information about the right to be forgotten upon request.

In certain circumstances, you have a right to request the restriction of processing of your Personal Data or to object to our processing of your personal data where we process it for our legitimate business interests or because it is necessary for the performance of a task carried out in the public interest or in the exercise of official authority. We may not be able to comply with such a request where there are legitimate grounds for the processing that override your interests, rights and freedoms or where the processing of Personal Data is required in connection with the defence, establishment or exercise of legal claims. You may also request the transfer of your Personal Data to another party.

You have a right not to be subjected to decisions that will have a significant impact on you based solely on automated decision-making including profiling, which produces legal effects concerning you or similarly significantly affects you. We may not be able to comply with such a request where we rely on your explicit consent or where it is necessary to enter and perform our contract with you. You may request a person to review the decision so that you can query it and set out your point of view and circumstances to us.

If you need to contact the Data Protection Officer, please contact us in writing at 4, Capital Quarter, Tyndall Street, Cardiff CF10 4BZ or via email: [DPO@pepper.money](mailto:DPO@pepper.money)

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 for access is clearly unfounded or excessive or we may refuse to comply with the request in these circumstances.

Where you may have provided your consent to the collection, processing and transfer of your Personal Data, you may have the right to withdraw your consent for that specific processing at any time. To withdraw your consent, please contact the DPO. Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law.

## 15. Keeping your Personal Data secure

We have appropriate security measures in place to prevent Personal Data from being accidentally lost or used or accessed in an unauthorised way. We limit access to your Personal Data to those who have a genuine business need to know it. Those processing your Personal Data will do so only in an authorised manner and are subject to a duty of confidentiality.

We also have procedures in place to deal with any suspected data security breach. We will notify you and any applicable regulator of a suspected data security breach where we are legally required to do so and in accordance with our legal obligations.

## 16. Use of your Personal Data by Credit Reference Agencies

We may supply your Personal Data to credit reference agencies (CRAs) and they will give us information about you, such as about your financial history. We may do this to assess creditworthiness, check your identity, trace and recover debts and prevent criminal activity.

We may also continue to exchange information about you with CRAs on an ongoing basis, including any debts not fully repaid on time. CRAs will share your information with other organisations. Your data will also be linked to the data of your spouse, any joint applicants or other financial associates.

They require us to pass on to you information about how they will use your Personal Data to perform their services or functions as data controllers in their own right. These notices are separate to our own.

The identities of the CRAs, and the ways in which they use and share Personal Data, are explained in more detail on their websites – clicking on any of these three links will also take you to the CRAIN document: TransUnion (formerly Callcredit) Privacy Centre ([transunion.co.uk](https://transunion.co.uk)); Equifax (<https://www.equifax.co.uk/crain>); Experian Credit Reference Agency Information Notice (CRAIN) | Experian. Please note: we accept no responsibility or liability for the contents of any third party website to which a hypertext link exists and give no representation or warranty as to the information on such websites.

## 17. How to complain

We hope that our Data Protection Officer can resolve any query or concern you raise about our use of your information. If not, you can contact the Information Commissioner at [ico.org.uk/concerns/](https://ico.org.uk/concerns/) or telephone: 0303 123 1113 for further information about your rights and how to make a formal complaint.

## 18. Changes to this Notice

We may amend this Data Protection Notice for Employees from time to time, in whole or in part, at our sole discretion, and any changes to this notice will be effective immediately upon publishing the revised notice.

If at any time we decide to use your Personal Data in a manner significantly different from that stated in this notice, or otherwise disclosed to you at the time it was collected, we will notify you, and you will have a choice as to whether or not we use your information in the new manner.

This notice was last updated on **16<sup>th</sup> May 2025**

If you have questions or concerns about this notice, please contact our Data Protection Officer.

## APPENDIX 1 - Fraud Data Bases

### General

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 Data 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. Cifas may allow the transfer of your personal data outside of the UK. This may be to a country where the UK Government has decided that your data will be protected to UK standards, but if the transfer is to another type of country, then Cifas will ensure your data continues to be protected by ensuring appropriate safeguards are in place.



## **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.