



Privacy Notice

For Job Applicants

International Personal Finance plc, Group of companies (IPF Group) is committed to the highest standards of ethical business conduct. We strive to achieve our business goals, whilst ensuring we do that in a responsible and lawful way. The lawfulness of the processing of our employee data remains at the heart of our conduct. This Privacy Notice describes the way we process your personal data, and also provides you with the information on your rights as a data subject as stated in the General Data Protection Regulation (GDPR), internal rules and policies as well as any applicable national laws.

Depending on the position you apply for, International Personal Finance plc or IPF International Limited, of Number Three Leeds City Office Park, Meadow Lane, Leeds LS11 5BD is your data controller. This means we are responsible for deciding how we hold and use personal information about you. This privacy notice applies to job applicants. This notice does not form part of any contract of employment and we may amend this notice at any time.

Your personal data might also be processed or controlled by other subsidiaries of the IPF Group, namely, but not limited to, Provident Polska S. A., Provident Financial Romania I.F.N. S.A., Provident Financial s.r.o., Provident Pénzügyi Zrt. and Provident Financial, s.r.o.

If your personal data is controlled by another controller from the IPF Group, the primary controller remains responsible for compliance of GDPR. In all cases, your contact point is the Data Protection Officer identified in this Privacy Policy. Irrespective of these arrangements, you may choose to exercise your rights towards any of the controllers from the IPF Group.



Contents

1.	Data Protection Principles	<u>p3</u>
2.	Identity and contact details of the Data Protection Officer	<u>p3</u>
3.	How our recruitment and selection process works	<u>p3</u>
4.	Personal data	<u>p3</u>
5.	How do we collect your data?	<u>p3</u>
6.	How long do we keep your data?	<u>p4</u>
7.	How do we protect your data?	<u>p4</u>
8.	To whom do we disclose your data?	<u>p4</u>
9.	How do we process your data?	<u>p4</u>
10.	How do we use your data and on what legal basis?	<u>p5</u>
11.	Your rights	<u>p8</u>
12.	Automated decision making	<u>p8</u>
13.	Your right to object to your data processing based on legitimate interest	<u>p8</u>
14.	Your right to turn to the Data Protection Authority or a competent court	<u>p9</u>
15.	Updates	<u>p9</u>

1 Data Protection Principles

We will comply with the data protection principles, which are that personal data will be:

1. Processed lawfully, fairly and transparently;
2. Collected only for a valid purpose which we have clearly explained to you and not used in any way which is incompatible with that purpose;
3. Relevant to the purpose we have told you about and limited only to those purposes;
4. Accurate and kept up to date;
5. Kept for no longer than is necessary for the purpose we have told you about;
6. Kept securely

This Privacy Notice provides you with transparent information about the personal data that we collect and how we use it and also informs you about your rights as a data subject and about the way you can exercise your data subject rights.

2 Identity and contact details of the Data Protection Officer

We appointed a data protection officer (DPO) who can be contacted with any privacy related issues.

e-mail: gdpo@ipfin.co.uk

or by post at the company address.

All matters will be treated confidentially however you may choose to contact the DPO anonymously.

How our recruitment and selection process works

Our recruitment and selection process is described in detail in our policy. For more information click [here](#).

3 Personal data

Personal data means any information which identifies you or could be used to identify you. We make sure that we only process your personal data strictly needed for a given purpose.

4 We might process the following categories of your personal data depending on the purpose followed:

Identification data – name, surname, address, national insurance number, identification document number, photograph, etc.

Contact data – email, telephone number, address, etc.

Data about professional life – employer, experience, position, salary, education, etc.

Data on credit history - existing loans, payment history, credit check, etc. Please see our Pre-employment screening policy for more information.

Financial data – income, assessable expenses, etc.

Digital data – cookies, IP address, websites and social network activities and other data publicly available on the Internet etc.

Special categories of data (sensitive data) – personal data revealing racial or ethnic origin, trade union membership, data concerning health. Please refer to our Policy on processing special categories of data for more information about how we collect and use this data click [here](#).

5 How do we collect your data?

Directly from you:

- In the recruitment and selection process.

From other sources:

- External company for the purpose of assessment of suitability during recruitment process
- External companies for the purpose of credit checks
- Occupational health or other health care providers e.g. GP
- Your former employer

6 How long do we keep your data?

As a general rule, we keep your personal data for the period necessary to reach the purpose of your data processing. It is in most cases the duration of the recruitment and selection process, and if you are unsuccessful, 6 months following. When we keep your personal data for another specific purpose, the storage period will be specified under the purpose in the section on how we use your data. Your consent would be required to extend data storage beyond this.

Any unsolicited CV's received will be destroyed or deleted.

[Please contact us for detailed information on how long we keep your data.](#)

7 How do we protect your data?

In order to make sure that your rights and freedoms are not put at risk and the compliance with relevant laws and regulations in the field of data protection are observed, we have implemented appropriate technical and organisational measures to ensure a sufficient level of security to the personal data processing.

These measures consist in regular training and testing of our employees and contractors, introduction of relevant policies and processes which are regularly reviewed and updated under the supervision of our Data Protection Officer. We also carefully assess our suppliers to ensure they adhere to GDPR requirements.

When we receive your electronic job application we store it securely with access limited to those involved in the recruitment process.

To whom do we disclose your data?

8 We only disclose your data to the extent necessary, and in a form that is required to achieve a given purpose.

Depending on the purpose of processing and need to meet our legal obligations and secure relevant expert knowledge in the processing activities, we might disclose your personal data to certain categories of third parties, namely:

- competent public bodies and authorities (e.g. investigative authorities, tax administrators, the Financial Supervision Authority, national insurance bodies)
- competent courts or tribunals
- other subsidiaries of the IPF Group
- our external consultants, assessment centres, auditors
- our external service suppliers (for example, benefit providers).

The disclosure will depend on:

- the purpose of processing
- the need to meet our legal obligations.

We only disclose your data to the extent necessary and in a form that is required to achieve a given purpose.

We may use external suppliers in the processing of data to either optimise our internal processes and/or conduct some of the processing on our behalf (typically to provide support and maintenance services). We process your personal data within the European Economic Area, and potentially also in other countries (to access the list of places of data processing please [click here](#)). For any occasion in which our suppliers process your personal data in countries which do not provide sufficient level of protection to your rights, we carefully assess the relevant circumstances and make sure appropriate safeguards are put in place so that your rights are not undermined. All of our suppliers who process your data outside the European Economic Area are required to sign the Module contractual clauses* and regularly check the level of security provided to personal data processed on our behalf. We ensure that conditions to enforce your rights and effective legal remedies are available. Any potential external supplier is subject to an internally conducted security pre-assessment, mutual rights and obligations are carefully addressed in the Data Processing Agreement.

* Commission Decision 2004/915/EC, dated 27 December 2004 – in which the Commission approved an alternative set of model clauses for transfers from data controllers in the EEA to data controllers outside the EEA. Commission Decision 2010/87/EU, dated 5th February 2010 – in which the Commission approved a new set of model clauses for transfers from data controllers in the EEA to data processors outside the EEA to replace the Set I controller to processor clauses.

How do we process your data?

We process your personal data in way of collection, storing and organising in our systems. We will compare and alter data to ensure it is accurate and kept up to date. When appropriate your data is destroyed/deleted. Within a course of our business activities as a multinational company we may transfer your personal data within the IPF Group in accordance with the legal data transfer requirements.

How do we use your data and on what legal basis?

Below we describe the legal basis for processing your data and different purposes of the processing. We would like to highlight that within our recruitment process you may go through different stages (applicant, short-listed applicant and successful applicant) which impacts the amount and types of data we have to process about you.

In order to protect your privacy we only require certain types of information from our short-listed applicants and successful applicants. Further details below:

We do not make fully automated decisions in our recruitment process.

- **Preparing to enter into an employment contract** - We will process your personal data set out above for the purpose of preparing to enter into the employment contract including, in particular, to assess your suitability for a role and, if you are successful and we make you a job offer, to set up and administer payments and benefits.

Retention period

For unsuccessful candidates we will keep your personal data only for the period of the recruitment process and for 6 months following the decision not to offer you employment. Your data is then destroyed/deleted.

- **To comply with our legal obligations and/or to assess your working capacity and/or for the purpose of occupational health** - Employment legislation and other applicable laws impose upon us legal obligations that necessitate the processing of your personal data.

As part of the recruitment process, **if you are a successful applicant**, we will ask you to complete a Health questionnaire to enable us to meet our legal obligations to ensure compliance with health and safety regulations at work, and provisions under equality act. Our Health questionnaire will be used by us for the purpose of alerting us to any health issues that may impact on your ability to carry out your role, including any disabilities or special needs, and which enable us to assess your working capacity and/or which may trigger the duty to make reasonable adjustments under the Equality Act.

We will also process data in order to check you are legally entitled to work in the UK.

We will only collect the information necessary for these purposes.

- **Based on our legitimate interests**

We also process your personal data based on our legitimate interest as long as your fundamental rights and freedoms do not override that legitimate interest. If we process your data based on our legitimate interest, we always identify such interest, make sure the processing is necessary to achieve that interest and carefully weigh your interests, rights and freedoms against our legitimate interest in a balancing test.

There are numerous situations where using your data is necessary for our recruitment and selection purposes, these would typically include:

- managing our relationship and interaction with you and other job applicants
- background checks and security vetting in recruitment and HR functions.

We might process all categories of your personal data as defined in the section Personal Data above for our legitimate interest, **except for special categories of data**.

- **We may also collect and process your data based on your consent.**

Your consent is voluntary and represents a specific, informed and unambiguous indication of your wish and can be withdrawn at any time. If we require consent, then at the relevant time we will provide you with all of the information necessary to carefully consider whether you wish to consent.

Special categories of data

Special categories of data require higher levels of protection. This is data which reveals race or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, health information, sexual life and sexual orientation.

We may process special categories of information in the following circumstances:

- In limited circumstances, with your explicit written consent.
- Where we need to carry out our legal obligations or exercise rights in connection with your employment.
- Where it is needed in the public interest, such as for equal opportunities monitoring.
- Where it is needed in relation to legal claims.
- Where it is needed to assess your working capacity, to obtain a medical diagnosis or for the purpose of preventive or occupational medicine.
- Where it is needed to protect your vital interests, or someone else's vital interests and you are not capable of giving consent.
- Where you have already made the information public.

We will use information about your physical or mental health or disability status to ensure your health and safety in the workplace and to assess your fitness to work, to provide workplace adjustments, to monitor and manage sickness absence and to administer benefits.

Social Media

We may check successful candidates on social media networks (e.g. LinkedIn) in the screening process. In doing so we only screen the social media profile of the job applicant which has manifestly been made public and which has been set up for business purposes. We only collect and process the data available to the extent that it is directly related to the performance of the job which is being applied for.

References

In order to confirm your previous work history we will ask for your written consent to provide, and for us to contact your chosen referees, which will include your most recent employer. If any inconsistencies or concerns are identified between the information provided by you and the references we receive, you would be given opportunity to provide an explanation.

Additional checks for high risk roles

To assess your suitability for roles that we have deemed high risk or where we are legally required to carry out checks by the regulatory authority and only in the event that you are a successful job applicant, we will request data to conduct the following:

- Identity check
- Adverse financial credit check
- Directorship check (directors only).

High risk roles have been identified as roles in which the role holder will have direct access to the company's strategic, and sensitive documentation and important financial information, as well as access to sensitive personal data relating to employees and job applicants and therefore the company needs to have the utmost confidence in the candidate's honesty and integrity. We have conducted a privacy impact assessment to ensure that your right to privacy does not override our reasons for conducting the checks.

Retention

The above additional checks are carried out by an external approved supplier. We will only record whether a check has yielded a satisfactory or an unsatisfactory result. The complete report will be held by the external company for a period of 18 months.

11 Your rights

Your numerous rights under the existing legislation have been summarised below. These are not absolute rights and there are exceptions. However,

- **You have a right to be informed about the data** we collect and how we use your data.
- **You have the right to access your personal data**, including the right to obtain a copy of your personal data we process. You are also entitled to ask for a copy of your interviewing notes.
- **You have a right to portability of your data** which you have provided to us, or data we process based on your consent and which is processed by automated means. We will provide you with that data in a secure Excel file, which is machine-readable, so you can store it or disclose it to other service providers. As the Excel file contains your personal data, please store the personal data securely on your device.
- **You may also provide your data obtained from other companies to us.** In addition you may request that we provide your personal data to another controller – however, we can only do that when the transmission is technically possible. We keep your personal data up to date, by asking you to review it from time-to-time and when required by law. However, if you find any data we have about you is incorrect, **you can request rectification of inaccurate data and you can have incomplete data completed** or additional data provided via contacts defined above. You can ask for restriction of your data processing if the accuracy of your personal data is contested for a period allowing us to verify the accuracy.
- **You have a right to restrict processing.** That means we will store your data, but not use it for anything else. You also have a **right to request erasure** of your personal data. You can exercise both rights on conditions specified by law. If you have obtained restriction of processing, you will be informed before the restriction of processing is lifted.
- **You have a right to contact us at any time**, if you believe your rights under data protection law have been violated.

Automated decision making

We do not make any automated decisions about you.

12 Your right to object to your data processing based on legitimate interest

Wherever we rely on our legitimate interest to use your personal data, we have taken into account and acknowledged your interests and rights under data protection law. Your privacy rights are always protected by sufficient safeguards and balanced with your rights and freedoms.

13 **If you wish to submit an objection or to exercise any of the rights referred to above click [here](#) or contact the DPO (details provided in the beginning of this Notice).** If your objection is sustained, it may stop us from processing your personal data for a given purpose.

14 Your right to turn to the Data Protection Authority or a competent court or tribunal

You have the right to contact the Data Protection Authority - Information Commissioner's Office, via the helpline on 0303 123 1113, from outside the UK +44 1625 545 700 or electronically via <https://ico.org.uk/global/contact-us/email/>, in writing at, Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow – Cheshire, SK9 5AF or another competent court or tribunal if you believe your rights with regards to the personal data processing have been violated.

Updates

15 We keep our privacy notice under review and may change it from time to time (mostly to comply with the law and data protection practices). Updated versions will be published on our webpage. This notice was last updated in April 2018.



International Personal Finance plc.

Registered address: Number Three, Leeds City Office Park,
Meadow Lane, Leeds, LS11 5BD. Registered in England and Wales.
Company Number 6018973