International Personal Finance

- Policy on processing special categories of data

INTERNATIONAL PERSONAL FINANCE PLC

Version:	April 2018
Status:	Issued
Owner:	Group Data Protection Officer
Date of printing:	24/05/2018
Date of Issue:	24/05/2018
Classification:	Internal

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 employees and job applicants data remains at the heart of our conduct. This Policy describes in detail the way we process special categories of data of our employees and job applicants.

We inform our employees and job applicants about the way we as a data controller process their data in relevant Privacy Notices. However, we are well aware of the fact that special category of data is personal data which the GDPR perceives more sensitive, and so need more protection as they could create more significant risks to a person's fundamental rights.

This Privacy Notice applies to current and former job applicants, employees, workers and contractors. This notice does not form part of any contract of employment and we may amend this notice at any time.

This policy should be read in conjunction with the Privacy Notice for Employees and Contractors, and the Privacy Notice for job applicants which can be found here.

WHAT ARE SPECIAL CATEGORIES OF DATA?

Special categories of data are data which provides information on:

- race;
- ethnic origin;
- political beliefs;
- religious or philosophical beliefs;
- trade union membership;
- genetics;
- biometrics (where used for ID purposes);
- health;
- sex life; or
- sexual orientation.

In general, processing of special categories of data is prohibited under the existing laws unless we qualify under one of the exeptions provided by the law.

We may process special categories of data 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 relation to legal claims.
- 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.

WHY DO WE PROCESS SPECIAL CATEGORIES OF DATA?

We might need to process the special categories of data for the following purposes:

MEDICAL QUESTIONNAIRE

As part of the recruitment process we ask successful job applicants to complete a Health questionnaire to enable us to meet our legal obligations to ensure compliance with health and safety regulations at work, to assess your working capacity and to comply with our obligations under the Equality Act. Our Health questionnaire will be used by us for the purpose of alerting us to any health issues that may impact potential and existing workers ability to carry out their role, including any disabilities or special needs, and which enable us to assess their working capacity and may trigger the duty to make reasonable adjustments under the Equality Act.

The Health questionnaire also gives us information about your physical or mental health or disability status to ensure your health and safety in the workplace and to provide workplace adjustments.

SICKNESS RECORD

Employment legislation and other applicable laws impose upon us legal obligations that necessitate the processing of health information, including the nature and length of any

sickness absence and medical reports obtained from your GP, consultant or occupational health, in order to monitor and manage sickness absence and to administer benefits.

WORK INJURY RECORD

Employment legislation, including health and safety legislation and other applicable laws impose upon us legal obligations that necessitate the processing of accidents and injuries at work.

SPECIAL CATEGORIES OF DATA PROCESSED FOR THE WHISTLEBLOWING PURPOSES

Since 2009 we run a 3rd party independent hotline and website whistleblowing scheme provided by our external supplier ExpoLink. The primary purpose is to enable the reporting of fraud and financial malpractice as required for UK listed companies by the UK Corporate Governance Code. Individuals call the ExpoLink hotline and make a report (which could contain PI about themselves & others). The ExpoLink operative takes details of the issue and a report is immediately sent to the relevant nominated contact at IPF plc. The report is investigated internally and conclusion of the investigation is relayed back to ExpoLink within specified timescales. The individual who reported the issue can call back and obtain the outcome. Data is only kept by Expolink long enough to relay reports and feedback. Individuals are encouraged to leave their details but reports can be made anonymously (however anonymous reporting is not encouraged) and the outcome obtained using a unique ID number. The processing was carefully assessed in a Data Protection Impact Assessment.

HOW DO WE PROTECT HEALTH INFORMATION?

In order to protect special categories of data of our employees and job applicants we have implemented appropriate technical and organisational measures to ensure a sufficient level of security to the personal data processing.

We may process special categories of data in both, paper and electronic form.All special categories of data in paper form is kept on the employee‘s file, which is kept in a fire resistant, high security locked filing cabinet. Access to the filing cabinets are resricted, with only two authorised employees having access to the file where they genuinely need access to

carry out their job. The access is assigned by the HR Director and is strictly role-based, given to the HR advisor and HR administrator. When an authorised person leaves the company or changes role within the company, the access rights are terminated.

All special categories of data processed in electronic form is kept in designated electronic files that has the same restricted access as detailed above.

The data may also be kept on our HR database, which is password protected and only roles in the HR team that are deemed to require full access to the system are able to gain access.

From time to time we might use external suppliers to process your data on our behalf. In such cases 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 data outside the European Economic Area are required to sign our model contractual clauses and we regularly check the level of security provided to personal data processed on our behalf. We ensure that conditions to enforce individuals 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.

Among the measures to protect special categories of data of our employees and job applicants we also conduct 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.

HOW LONG WE STORE THE DATA?

As a general rule, we keep personal data for the period necessary to reach the purpose of the data processing activity. Detailed information on how long we keep your data you can find in our Retention policy here.

When we collect the Medical Questionnaire we store it securely with access limited to those involved in the recruitment process for a period of the employment relationship and 6 years after the relationship termination.

We process work injury related data for a period of the employment relationship and 6 years after the relationship termination.

We process the data on sickness leave for a period of the employment relationship and 6 years after the relationship termination.

We process the data gained during the whistleblowing scheme running for a period of 3 months once the case is closed.

After the retention period expires, the data is securely destroyed or deleted in compliance with our internal policies.

DATA PROTECTION PRINCIPLES

In processing special categories of data we make sure the data protection principles are duly observed.

LAWFULNESS, FAIRNESS AND TRANSPARENCY

To process special categories of data lawfully, we make sure we have a legal ground for processing the data. To make sure we process the data fairly and transparently, we provide individuals with detailed information information on the processing activities in the Privacy Notice and other relevant polices, including allowing the individuals to excercise their data protection rights.

PURPOSE LIMITATION

We only process data for a valid purpose which we have clearly explained and not use data in any way which is incompatible with that purpose.

DATA MINIMISATION

The processing of personal data is limited to the personal data that is relevant, necessary and adequate for a given purpose.

ACCURACY

We only process accurate and up to date data. We always properly verify the authentication of your personal information.

STORAGE LIMITATION

The data we process is kept for no longer than is necessary for the purpose we process the data for. The relevant retention periods are described in detail in the IPF Retention policy and in the above section: *How long we store the data*.

SECURITY

In order to make sure that individual´s rights and freedoms are not put at risk and that compliance with relevant laws and regulations in the field of data protection is observed, we have implemented appropriate technical and organisational measures to ensure a sufficient level of security to personal data processing. These measures include; regular training and testing of our employees and contractors, introduction of relevant internal 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.

Where possible data security enhancing techniques are used such as encryption so that appropriate security of the data is ensured.

As a general rule, we make sure your personal information is treated with respect, kept up to date and correct and we don't process any irrelevant or excessive information.

IDENTITY AND CONTACT DETAILS OF THE DATA PROTECTION OFFICER

We, International Personal Finance plc, of Number Three Leeds City Office Park, Meadow Lane, Leeds LS11 5BD, work as your personal data controller.

We have an appointed Data Protection Officer (DPO) whom you may contact with any privacy related issues: gdpo@ipfin.co.uk or by post at the company address.

All matters will be treated confidentially; however you may contact our DPO anonymously.

Updates

We keep this policy regularly updated to comply with the law and data protection practices. Updated versions will be published on our webpage. This policy was last updated in May 2018.