Data Protection Policy

Associated risk category:	GD – Data Protection and Privacy
Policy owner:	Group Data Protection Officer
Version:	2.0
Last review date:	May 2023
Approval body:	Chief Legal Officer
Next review date:	May 2024

Contents

1. About this Policy

To perform its business activities and manage its operations IPF Group needs to process Personal Data. This means it is responsible for deciding how personal information about individuals is collected, used and retained. Personal Data may include information about customers, employees, contractors, customers representatives or other people IPF Group has a relationship with.

This policy defines the IPF Group governance model for handling Personal Data, to ensure it is dealt with in a lawful way, setting out the principles and standards required through the applicable legislation in the UK or other jurisdictions, including the General Data Protection Regulation ("GDPR").

2. Policy Purpose

The objective of this policy is to ensure that all reasonably practicable steps are taken to ensure IPF Group:

- Complies with data protection and privacy legislation and processes data lawfully;
- Protects the rights and freedoms of customers, employees, and any other individuals with whom it has a relationship;
- Protects itself from the risk of non-compliance with data protection legislation, including the GDPR, or other rules, regulations or requirements relating to privacy which apply to the IPF Group.

3. Policy Scope

This policy applies to all employees, customer representatives and contractors working for or on behalf of the IPF Group and to the processing of all data it holds relating to such identifiable individuals.

4. Definitions

The following definitions are used in this policy:

Definition	Meaning
Data Protection Framework	means the IPF Group-wide governance model on dealing with privacy related matters consisting of this Policy and related procedures, guidelines and/or instructions such as the ones regarding data breaches, third party risk (suppliers), data retention, data subject requests, privacy impact assessments, data transfers, risks' identification, assessment, reporting as well as design and assessment of appropriate controls.
Personal Data	means any information relating to an identified or identifiable natural person ("data subject" or "Individual"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
Processing Personal Data	means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Personal Data Breach	means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.
IPF Group	means INTERNATIONAL PERSONAL FINANCE PLC, with its registered office at 26 Whitehall Road, Leeds LS12 1BE, United Kingdom, company number 6018973 and all companies in which International Personal Finance plc directly or indirectly owns or controls the voting rights attaching to not less than 50% of the issued share capital or controls the appointment of a majority of the board of management.
GDPR	means REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 („EU GDPR“) –AND/OR same regulation as transposed into United Kingdom national law by operation of section 3 of the European Union (Withdrawal) Act 2018 and as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 ("UK GDPR").

5. Policy Requirements and Appropriate Conduct

5.1. Data Protection Principles

IPF will manage data protection in line with its Data Protection Principles. These outline the basic responsibilities for all the IPF Group in relation to this area and guide all the activities undertaken by the Group relating to the management and use of Personal Data. These Principles enable the Group to handle information in line with the expectations of our customers and broader regulatory requirements.

The Data Protection Principles are:

- Transparency – To be open and transparent about what we do with Personal Data and why we use it.
- Purpose Limitation – To collect and process Personal Data data for specific business purposes.
- Lawfulness – To ensure Personal Data is processed only where legally allowed.
- Data Minimisation - To collect and use Personal Data only to the minimum degree necessary.
- Data Accuracy - To keep Personal Data accurate, complete and up to date.
- Storage Limitation - To not keep Personal Data longer than necessary.
- Security and Confidentiality of Data – To protect Personal Data from unauthorised loss, alteration, disclosure, or access; to disclose Personal Data to third parties only in accordance with this Policy.
- Accountability – To ensure our processes relating to Personal Data comply with this Policy

5.2. Individuals' Rights

We **PROTECT INDIVIDUAL'S RIGHTS** to:

- **Access** the data processed about themselves.
- **Be informed** about the processing operations.
- **Obtain,** move, copy, have data transmitted **and/or reuse** Personal Data, under certain circumstances.
- Have data **changed, amended, or rectified** if inaccurate or incomplete, **deleted or removed** upon request.
- **Restrict** Personal Data processing, under specific circumstances.

- **Object** to data being processed, under specific circumstances, including the right to withdraw their consent.
- **Object to automated decisions** and ask for human intervention.
- **Lodge a complaint** with us, with data protection authority or a court if they are unsatisfied with the way we process their data.

These are not absolute rights and there are exceptions. These rights may also vary from jurisdiction to jurisdiction, based on applicable laws.

5.3. Managing data protection risk

AT GROUP LEVEL, we manage data protection through a range of both Group and market actions. At Group level, the Group Data Protection Officer is responsible for

i. advising the Group of its obligations under GDPR;
ii. monitoring compliance with this Policy including monitoring training and oversight activities related to data protection compliance;
iii. producing, on an annual basis, a Privacy Plan which is designed to ensure the Group complies with relevant data protection requirements;
iv. acting as the Group Risk Owner for Data Protection Risk;
v. maintaining an appropriate data protection framework which reflects the principles detailed in this Policy.

At LOCAL LEVEL, markets are responsible for developing their own data protection frameworks aligned with the IPF Group's Data Protection Framework along with procedures which are in accordance with IPF Group standards. Each market is responsible also for monitoring and ensuring compliance with this Policy and with all applicable local legislation, regulation, and policies.

To implement these requirements, each market must

i. have a Local Data Protection Officer in place, who is responsible for ensuring that each market has an appropriate policy, which reflects both the standards detailed in this Policy and local legal and regulatory requirements.
ii. Acting as Local Risk Owner for Data Protection Risk;
iii. collate numbers of customer' complaints concerning potential breaches of relevant and applicable data protection and privacy legislation;
iv. collate number of Personal Data Breaches.

Each Local Data Protection Officer reports to the Legal Director for their market and with a dotted line to the Group Data Protection Officer. Responsibility for compliance with relevant laws and regulations in every market, including GDPR, as applicable, ultimately rests with the senior management of each entity forming part of the IPF Group.

5.4. Risks and Controls

Data Protection Risk is a "Key Risk" as defined in the IPF Group's Enterprise Risk Management Framework. This Framework sets how assessment data protection risks for individual markets and Group are undertaken. Data protection controls and key performance metrics design are reviewed on an annual basis and are regularly assessed (on a quarterly basis).

The following principles should be applied in the selecting and implementation of data protection controls:

Commensurate with the risks faced by the individuals and the company operating the controls	Appropriate for the nature, size and maturity of the business	Tailored to the local operational and regulatory environment	Scalable to accommodate future growth where possible	Aligned to the group data protection framework

5.5. Personal Data Breaches

A Data Breach Procedure is developed and implemented under the responsibility of Group Data Protection Officer. The Data Breach Procedure provides guidance on what amounts to a Personal Data breach, how any such breach should be addressed in compliance with requirements set out in the relevant and applicable legislation, methodology on how to assess severity of such an incident, what is the data loss reporting process for reporting of Personal Data breaches internally and address any legal requirements in terms of external notifications as well, if the case.

Local markets DPOs are responsible to develop and implement a local Data Breach Procedure, in line with this procedure, Data Breach procedure delivered by GDPO, and other relevant and applicable legal and business requirements.

All employees, customer representatives and contractors must immediately report actual or suspected Personal Data breaches he/she is witnessing or if he/she inadvertently causes one themselves to appointed staff in this respect including Data Protection Officer, according to the local data protection framework rules and the Data Protection Procedure.

Data Protection Officer shall document any Personal Data breaches and shall manage it according to the other relevant internal rules respectively this procedure, the Data Breach Procedure (including Data Loss Reporting Process).

5.6. Training and Awareness

IPF Group provides induction training and annual refresher trainings and awareness sessions on this Policy and related confidentiality and data protection obligations to all staff members who have access to Personal Data.

Specialised training is provided to specific functions considering the level of data protection risk and need for awareness in those areas. Responsibility for developing and delivering such training sits with the Group DPO and Local DPOs for specific markets.

5.7. Privacy by Design

The Group will look to implement privacy-by-design measures when processing Personal Data, by implementing appropriate technical and organisational measures (like pseudonymisation) in an effective manner.

The Group will ensure therefore that by default, only Personal Data which is necessary for a specific purpose is processed.

5.8. Data Privacy Impact Assessment

The Group will conduct DPIAs in respect of high-risk processing before that processing is undertaken and in particular in the following circumstances:

(i) the use of new technologies (programs, systems or processes), or changing technologies (programs, systems or processes);
(ii) automated processing including profiling;
(iii) large scale processing of sensitive (special category) data.

A DPIA must include:

(i) a description of the processing, its purposes and the Data Controller's legitimate interests if appropriate;
(ii) an assessment of the necessity and proportionality of the processing in relation to its purpose;
(iii) an assessment of the risk to individuals; and
(iv) the risk-mitigation measures in place and demonstration of compliance.

5.9. Third Parties (Suppliers). Data Transfers

We manage data protection third party risk when working with suppliers who process Personal Data by carrying out due diligence through internally conducted pre-assessments to ensure that appropriate safeguards are in place, with mutual rights and obligations carefully addressed in Data Processing Agreements.

Principal duties for all employees, customer representatives and contractors in what regards procurement activities involving any type of use of Personal Data, and in any amount, are set in Group Procurement Policy. More detailed responsibilities and instructions are set in the Data Protection Procedure.

We also make sure that the requirements for transferring Personal Data to third parties outside IPF Group are met.

In many of our markets there are restrictions on data transfers to other countries. Such data transfers may only happen if they are compliant with applicable law and regulation.

6. Roles and Responsibilities

IPF Group Board	• Responsible for setting the overall direction and commitment to data protection compliance, determining the nature and extent of the principal risks the IPF Group is willing to take to achieve its long-term strategic objectives and providing sufficient resources to enable the effective performance of these objectives. IPF Board may delegate its powers regarding data protection and privacy area to the Audit & Risk Committee.
Local Board and Country Manager (CEO)	• Responsible for setting the overall direction and commitment to data protection compliance for the local market, determining the nature and extent of the principal risks is willing to take to achieve its long-term strategic objectives and providing sufficient resources to enable the effective performance of these objectives.
Local Legal Director	• identifying relevant legislation relating to data protection, assessing its impact to the business and reporting this assessment to the local Board and Country Manager. • ensuring the market discharges its regulatory and legal responsibilities relating to data protection in line with the provisions of the Group Risk Appetite Statement. • ensuring the response to any Personal Data Breach complies with relevant policy requirements. • creating an appropriate culture of compliance. • overseeing and reviewing data protection compliance and risk status and determining market risk appetite • ensuring appropriate resources for the data protection function. • ensuring the IPF Group Privacy Plan is appropriately followed • providing updates on compliance status and market data protection issues to Group.
(Group) Data Protection	• managing the requirements arising from this IPF Group Data Protection Policy including updating it when necessary. • informing and advising employees of their obligations pursuant to applicable data protection/privacy legislation.

Officer (GDPO/ DPO)	• recommending corrective actions for market issues and future data protection strategy • continuously monitoring compliance with relevant legislation including GDPR as applicable and with the policies of the IPF Group in relation to the protection of Personal Data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits. • cooperate with the competent supervisory authority and act as the contact point for the supervisory authority on issues relating to Personal Data. • act as a contact point for data subjects, where they choose to contact the DPO, with regard to all issues relating to processing of their Personal Data and exercise of their rights. • provide advice in conducting data protection impact assessments where required. • report data privacy relevant matters (including privacy incidents) on a regular basis to the Chief Legal Officer, the local Board and GDPO as applicable. • performing other duties as required to promote the Data Protection Principles (e.g. ensuring local staff are trained and a culture of privacy awareness is created, holding records as required). In the performance of his/her duties, the DPO is responsible to have due regard to the risk associated with the processing operation, taking into account the nature, scope, context and purposes of processing.
Heads of Function Owning Business Change/PMO	Accountable to develop change and product management processes that include applicable data protection and privacy requirements, namely lawfulness, fairness and transparency, privacy by design and by default, data minimisation, purpose limitation, storage limitation, accuracy, integrity, and confidentiality and where needed, the DPIA is conducted, and consulted with the Local DPO or GDPO, before a new or changed product or process (entailing any type of use or access to Personal Data) is launched.
Head of Function owning the business process (Process Owner/ Owner of Business Activity)	Usually the head of the function(s) in which the process (entailing any type of use or access to Personal Data) takes place. The process owner is responsible for implementing adequate controls to ensure that the data protection rules are applied according with this Policy and the standards as defined by the data protection framework.
Everyone	All employees, customer representatives and contractors must comply with this Policy. This includes staying alert to potential sources of data protection or privacy risk and complying with the specific requirements outlined in this document. Everyone must immediately report actual or suspected Personal Data breaches and breaches of this Policy, according to the Personal Data Breach Procedure. All employees, customer representatives and contractors shall be authorized to access Personal Data only to the extent necessary for the applicable legitimate business purposes for which the data are processed by IPF Group and to perform their job. All employees, customer representatives and contractors who access Personal Data must meet their confidentiality obligation and observe strictest confidentiality with respect to the Personal Data it collects,

	processes, or accesses as a result of the performance of his/her job, and refrain from disclosing it to any other natural or legal person, including co-workers and other staff members, where the latter are not expressly authorised to access such data by virtue of instructions of the employer, contract or law. Employee will hold the confidential information consisting of Personal Data received in strict confidence and will exercise a reasonable degree of care to prevent disclosure to others. All employees, customer representatives and contractors should request assistance and advice from their line manager or Local DPO if they are unsure about any aspect of the protection of Personal Data. All employees must undergo mandatory data protection training. All employees must regularly review all the systems and processes under their control to ensure they comply with this Policy.

7. Policy governance

Further details on how the principles detailed in this Policy including how this risk is managed and governed, roles and responsibilities, transfer of Personal Data to third parties, procedure on handling Personal Data breaches or data subject rights are set in the Data Protection Procedure maintained by the Privacy Function.

7.1. Breaches and Exceptions to Policy

Exceptions to Policy Breaches	Should a breach in this policy be identified, via any means, it must be reported to the Local DPO and Group DPO. Any deliberate breach of this policy may be considered a disciplinary offence and may result in the termination of a customer representative's or employee's agreement/contract.
Whistleblowing	If for any reason you are uncomfortable reporting a breach as requested above you can access our independent whistleblowing services at https://report.whistleb.com/en/ipf for European, IPF Digital or Group related matters or https://hacerlocorrecto.ethicsglobal.com/ for Mexico.

7.2. Assurance

Owner	This Policy is owned by Legal Department – Data Privacy – Group Data Protection Officer.
Assurance mechanisms and Internal Audit	The requirement to ensure this policy is correctly applied to individual markets falls with the local Legal Directors supported in this role by the local Data Protection Officer. To ensure compliance with the policy, oversight is provided by the Group Data Protection Officer reporting to the Group Chief Legal Officer. Group Data Protection Officer annually reports to the IPF Board or Audit & Risk Committee as delegated by the IPF Board.

8. Related Policies

Group Responsible Procurement Policy	Sets main rules of managing relationship with suppliers in compliance with data protection legal obligations and internal demands.
Group Information Security End User Standards	Sets standard and rules to ensure an adequate level of information security, including protecting Personal Data against threats so that confidentiality, integrity, and availability are ensured through appropriate technical and organisational measures implemented in the information systems or within business operations.
Group IT Security Policy	describes the Group IT Security policy and provides a framework for IT security processes, standards and mechanisms. It defines the security objectives and fundamental principles (like availability, integrity, confidentiality, non-repudiation), for securing IT and information assets in accordance with business goals and sets minimum requirements for local markets.
Group Risk Management Policy	Sets risk management internal rules applicable also to data protection area.
Group Internal Control Policy	Sets internal control requirements applicable also to data protection area.
Business Continuity Policy	Ensures business continuity, including availability of Personal Data.
Dawn Raid Policy	Dawn Raids may be conducted by a number of relevant authorities including, in the UK, the Information Commissioner's Office or any equivalent regulators or authorities in the markets in which the IPF Group operates.