Policy: Data Privacy

1. Objective

As part of its business operations, IBS is committed to comply with applicable data protection laws. This Data Privacy Policy (Policy) applies to all companies of IBS group including IBS Software Private Limited, its parent, subsidiaries and affiliated companies (IBS). All employees of IBS are expected to handle Personal Data with care. In particular, all Personal Data shall be processed and the security and confidentiality of all Personal Data shall be maintained, in accordance with applicable laws and regulations.

The capitalized terms which are used in this Policy are explained in Appendix 1.

Key objectives of this Policy are to:

- Establish a defined framework aligned to the generally accepted privacy principles (GAPP) and applicable laws and regulations (including General Data Protection Regulations (EU 2016/679) to ensure privacy and protection of the Personal Data handled at IBS.
- Integrate with the Information Security Policy of IBS, to safeguard against identified risks of Personal Data Breach
- Effectively monitor and address changes in IBS environment Processing Personal Data.

2. Scope

This Policy shall apply to:

- all Data Subjects who provide their Personal Data to IBS such as employees, job applicants, contingent workers, interns, retirees, contractors, customers, Suppliers, business partners, shareholders etc.;
- all locations where the IBS operates and where Personal Data is collected from; and
- all methods of collecting, storing and processing Personal Data.

2.1 Applicability of local law

Data Subject shall retain any rights and remedies they may have under applicable local law. This Policy shall apply only where it provides supplemental protection for Personal Data. Where applicable local law offers Data Subjects more protection than this Policy, then the local law shall apply. However, where this Policy provides more protection to the Data Subjects than applicable local law or provides additional safeguards, rights or remedies for Data Subject, then this Policy shall apply.

Due to the differences in regulations among the jurisdictions that IBS operates in, IBS has adopted this Policy which creates a common code of values, policies and procedures intended to achieve nearly universal compliance. This Policy will be supplemented with alternative or additional policies or implementation procedures for a specific jurisdiction if required.

The Data Protection Office may publish additional guidelines that apply for specific countries. Where such additional guidelines are published, those policies shall take precedence over this Policy with respect to those particular countries/regions.

Where there is a question as to the applicability of this Policy, employees shall seek the advice of the Data Protection Office prior to Processing of any Personal Data.

3. Policy

3.1 Principles for Processing Personal Data

IBS shall Process Personal Data only if such Processing falls within the scope of the principles listed below;

Fairness and lawfulness

When Processing Personal Data, the rights of the Data Subjects must be protected. Personal Data must be Processed in a legal and fair manner.

Restriction to a specific purpose

Personal Data can be processed only for the purpose that was expressly consented by the Data Subject and for no other purpose. Changes to the purpose subsequent to the collection of Personal Data will require additional consent from the Data Subject prior to Processing.

Data reduction

Before Processing Personal Data, the Processor must determine whether and to what extent the Processing of Personal Data is necessary in order to achieve the purpose for which the Personal Data is collected

Data Accuracy

Data Subject shall have a responsibility to provide accurate, complete and relevant information in order to maintain the quality and integrity of all Personal Data. Data Subject may contact IBS designated personnel as detailed in Appendix 2, for any updates or corrections to their Personal Data. Data Subject may verify and challenge the accuracy and completeness of their Personal Data and have it amended, if inappropriate. Upon request by the Data Subject, IBS shall take commercially reasonable steps to ensure that all such inaccurate or incomplete Personal Data are corrected, supplemented or updated.

Data Retention

IBS does not retain Personal Data any longer than is necessary to meet the purpose. The retention period for Personal Data is determined by and shall be the longer of:

- the purpose for which the Personal Data was collected and fulfilment of that purpose;
- any contractual retention period in relation to such Personal Data; and
- retention period required under any local laws.

Data Security

With respect to any Personal Data, IBS shall take appropriate physical, technical, and procedural measures in accordance with IBS Information Security Policy to:

- prevent and/or to identify unauthorized or unlawful Processing of Personal Data,; and
- prevent accidental loss or destruction of, or damage to, Personal Data

Data Transfer

Any transfer of Personal Data out of a region (such as European Economic Area, DIFC etc.) or a country (such as Australia, Singapore etc.) from where it is collected shall be performed in compliance with local privacy laws and with adequate protection. In such cases the Processor shall seek advice of the Data Protection Office prior to transfer of any Personal Data.

3.2 Reliability of data Processing

Processing Personal Data is permitted only under the following legal basis.

Consent to data Processing

Consent of the Data Subject shall be obtained prior to Processing any Personal Data. In scenarios where IBS is a Data Processor, it is the responsibility of the Data Controller to collect the consent from the Data Subject before sharing the Personal Data with IBS. Consent must be a positive indication and cannot be inferred from silence, inactivity or pre-ticked boxes. Consent will only be accepted where it, specific, informed and an unambiguous. Where consent is given, a record will be kept documenting how and when consent was given. The consent may be withdrawn by the Data Subject at any time and once notified of such withdrawal, IBS shall stop Processing Personal Data relating to such Data Subject.

Processing Sensitive Personal Data

IBS shall Process Sensitive Personal Data or 'special categories of Personal Data' only to the extent necessary to serve the applicable legitimate purposes. Sensitive Personal Data can be Processed only if the law requires this or the Data Subject has given express consent. If any of IBS business units intends to process any Sensitive Personal Data, the Data Protection Office must be notified in advance in writing, so that Data Protection Office can advise business unit if any additional security measures needs to be implemented and business units shall implement any additional security measures advised by the Data Protection Office with respect to Processing of such Sensitive Personal Data.

Data Processing for a Contractual Relationship

Personal Data of any prospects, customers, Suppliers and partners can be Processed in order to establish, perform and terminate a contract. Prior to execution of a contract, Personal Data may be processed to prepare bids or purchase orders or to fulfill other requests of any such prospect, customer, Supplier and partner. During the contract preparation process and during the lifecycle of a contract, prospects, customers, Suppliers and partners may be contacted using the information that they have provided. Any restrictions clearly conveyed in writing by the prospects, customers, Suppliers and partners shall be complied with.

Data Processing for Employment Relationship

In employment relationships, Personal Data shall be Processed based on the purposes notified to employees in the Employee Consent Form. If in case the scope of IBS Processing of Personal Data changes, the Employee Consent Form shall be updated appropriately and obtain signoff from employees.

During recruitment process, the applicants willingly share their Personal Data, for seeking candidature in the recruitment process. ' Personal Data may be processed for determining the applicant's suitability for employment. If the applicant is not found suitable for any immediate positions available, the Personal Data may be retained in the candidate database for re-considering their candidature in future. During the period for which such Personal Data is retained, the head of IBS recruitment team will make sure that the Personal Data is not used for any purpose other than recruitment.

Data Processing for advertising purposes

Personal Data may be Processed for advertising purposes or market and opinion research, provided that this is consistent with the purpose for which the Personal Data was originally collected. The Data Subject shall be informed about the use of his/her Personal Data for advertising purposes and shall have consented to such use. If the Data Subject refuses the use of his/her Personal Data for advertising purposes, it shall not be used for these purposes. Any other restrictions from specific countries regarding the use of data for advertising purposes shall also be observed.

Automated individual decisions

If IBS engages in any decision making based solely on the automated application of predetermined rules, the same shall be disclosed to the Data Subjects or Data Controller, as applicable.

Use of Personal Data in websites

If Personal Data is collected, processed and used on IBS websites the Data Subjects shall be informed of this in a privacy statement that shall include information about cookies used in the websites. If user profiles are created to evaluate the use of websites and apps, the Data Subjects must always be informed accordingly in the privacy statement. Personal tracking may only be effected if it is permitted under local law or upon consent of the Data Subject. The Data Subject shall be given the option to opt out from promotional emails in the privacy statement.

Telecommunications and internet

IBS may provide telephone equipment, e-mail addresses, intranet and internet along with internal social networks to its employees primarily for work-related assignments. Such employees shall ensure that the Personal Data accessible to them as part of their work shall be used only for its intended purpose.

Cross Border Data Transfer

Personal Data may be transferred by IBS where any of the following conditions apply:

- The Data Subject or Data Controller, as applicable has given consent to the proposed transfer;
- The transfer is necessary for the conclusion or performance of a contract signed between IBS and a customer or Supplier;
- The transfer is necessary in order to protect the vital interests of the Data Subject;
- The transfer is required by law;
- The transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise, or defense of legal claims;

Transfer of Personal Data across borders shall be performed in compliance to the following procedures:

- Data subjects or Data Controller, as applicable shall be clearly notified of any transfer of Personal Data across borders of the country in which the information was collected.
- Personal Data shall not be transferred to another entity, country or territory, unless reasonable and appropriate steps have been taken to maintain the required level of data protection.
- Personal Data may be communicated to third persons only for reasons consistent with the purposes for which the data were originally collected or other purposes authorized by law.
- All Sensitive Personal Data transferred shall be de-identified or shall be protected against unauthorized access by use of standard encryption techniques.
- All transfers of Personal Data to third persons for further Processing shall be subject to written agreements. The Data Protection Office shall, in cooperation with the IBS Legal Department, develop standard terms and conditions which can be used for this purpose.
- EU Personal Data shall not be transferred to a country or territory outside the European Economic Area unless the transfer is made to a country or territory recognized by the EU as having an adequate level of legal protection for the rights and freedoms of Data Subjects in relation to the Processing of Personal Data, or is made in compliance with one of the mechanisms recognized by the EU (such as use of model contracts/ BCR's) as providing adequate protection when transfers are made to countries or territories lacking an adequate level of legal protection.

- For non EU regions, transfers to another country or territory shall be performed in compliance to the above procedures or specific regulations mandated by local law (such as notifying and obtaining approval from the local privacy regulator/ governing body, where applicable, and mandated by law)

3.3 Data Privacy Roles of IBS

IBS will be Data Controller for employees, job applicants, contingent workers, interns, retirees, contractors, customers, Suppliers, business partners, shareholders etc. Aligning with the Privacy Principles, IBS has obligations to obtain and record consent, privacy impact assessment, contracts with PII processors, providing information to PII principals, mechanism to modify and withdraw consent, and handle requests from PII principals.

For all Customer Contracts, IBS will be a Data Processor. Aligning with the Privacy Principles, IBS has obligations to obtain customer agreement on PII processing, support the customer to fulfill his obligations to the PII Principals and handle PII as agreed in the contract between IBS and the Customer. IBS will alert the customer in case of any instructions from them that would infringe the privacy compliance.

3.4 Data Classification

- Personally Identifiable Information (PII) – information that can be used on its own or with other information to identify, contact, or locate a natural person, or to identify an individual in context. e.g., Name, Address, Phone Number, IP Address etc.
- Sensitive Personally Identifiable Information (SPII) – information that reveal an individual's racial or ethnic origin, political opinions or membership in political parties or similar organizations, religious or philosophical beliefs, membership in a professional or trade organization or union, physical or mental health including any opinion thereof, disabilities, genetic code, addictions, sexual orientation, criminal offences, criminal records, proceedings with regard to criminal or unlawful behaviour, or social security numbers issued by the government, or any other type of data that qualifies as Sensitive Personal Data under applicable local law.

Any data that does not fall under the above classification will not come under the purview of Data Privacy.

3.5 Data Protection Impact Assessments (DPIA)

IBS will ensure that the privacy impact assessment of all customer contracts including any new contract is done starting from the contracting stage.

IBS will ensure that impact analysis done during contracting phase include the following:

- Classification of data involved, to identify Personal Data
- Processing of personal data
- Rights of data subjects

Where a new requirement is triggered from a customer, the privacy impact assessment will be performed as part of the process for Requirements Management.

Periodically, IBS will conduct privacy impact assessment to incorporate the changes in the regulatory environment.

3.6 Data Privacy Request Management

IBS will accept and process data privacy related requests from its data subjects in compliance with relevant data privacy laws, as per the Data Privacy Request Handling process

IBS will ensure that the service time for all requests related to data privacy are tracked to ensure compliance with relevant data privacy laws.

If IBS receives a request related to data privacy from a data subject for whom IBS is not the Data Controller, then IBS will make all possible efforts to identify the respective data controller and forward the request to the data controller.

3.7 Privacy Information Management System

IBS will operate a Privacy Information Management System conformant to the ISO 27701:2019 standards and relevant data privacy laws, for Privacy Management in the collection, processing and storage of personal data in business operations. It will be part of the IBS Quality System.

3.8 Data Breach Management and Notification

The term 'Personal Data Breach' refers to a breach of security which has led to the destruction, loss or any unauthorized alteration, disclosure or access to Personal Data. Failure to comply with any applicable privacy laws will also constitute a Personal Data Breach.

Where a breach is likely to result in a risk to the rights and freedoms of individuals, the relevant supervisory authority must be informed by the Data Controller. Where IBS is not the Data Controller, IBS will notify the Data Controller in writing. All notifiable breaches will be reported to the relevant supervisory authority within 72 hours of IBS becoming aware of it. The risk of the breach having a detrimental effect on the Data Subject, and the need to notify the relevant supervisory authority, will be assessed on a case-by-case basis.

Effective and robust breach detection, investigation and internal reporting procedures are in place at IBS, which facilitate decision-making in relation to whether the relevant supervisory authority, customer or the public need to be notified.

Within a breach notification, the following information will be outlined:

- The nature of the Personal Data breach, including the categories and approximate number of Data Subject and records concerned
- An explanation of the likely consequences of the Personal Data breach
- A description of the proposed measures to be taken to deal with the Personal Data breach
- Where appropriate, a description of the measures taken to mitigate any possible adverse effects
- The name and contact details of the DPO

In many countries, misuse of Personal Data, may lead to criminal prosecution and may result in claims for compensation or damages. Individual employees will be responsible for any such violations and it may lead to sanctions under employment law.

3.9 Security of Personal Information

Implementation of adequate physical & technical security controls:

- Physical, technical, and organizational measures to ensure the security of Personal Data shall be in accordance with IBS Information Security Policy.
- Data Protection Office shall assess the security measures implemented to safeguard Personal Data on a regular basis and recommend update of the security measures, where required.
- Employees Processing Personal Data shall be imparted with additional job-specific privacy training (e.g., Training on Embedding Privacy in Software Development etc.)

Access to Personal Data

- Staff accessing Sensitive Personal Data or Personal Data, as part of their job responsibility, shall adhere to the Non-Disclosure Agreement (NDA) signed at the time of joining the organization and any subsequent changes to it.

- Staff shall not disclose or use aforementioned data for personal / economic use.
- Staff shall take utmost care considering the sensitivity of the Personal Data.
- Staff shall not save the Personal Data on the local desktop or laptop.
- Staff shall not take unnecessary printouts of aforementioned data. If printed, the hardcopy should be securely stored, so as not to knowingly or unknowingly disclose it to unauthorized persons. Print copies, if any, should be destroyed, by shredding it, immediately after use.

Privacy Incident Management:

- IBS shall formulate and implement an incident and breach management mechanism to ensure that exceptions in data privacy compliance are promptly reported to the Data Protection Office.
- All employees shall be aware of the mechanism of reporting privacy incidents.
- Data protection Office shall investigate the incidents and track it to closure. Data Protection Office shall maintain a history of such incidents.

Employee Confidentiality Agreements

- Confidentiality agreements and NDA's shall be signed by all employees and contractors on or before their joining date.
- All such persons involved in any stage of Processing Personal Data shall explicitly be made subject to a requirement of secrecy which shall continue after the end of the employment relationship.

Privacy Training

- All IBS employees and contractors shall mandatorily undergo the Privacy training during onboarding into IBS and on an annual basis.
- Training attendance records shall be maintained by the HR Department.
- Training material shall be reviewed by the Data Protection Office on an annual basis and updated, if necessary.
- DPO Team and DP Champions will regularly upskill themselves through training and other means to ensure the upkeep of PIMS

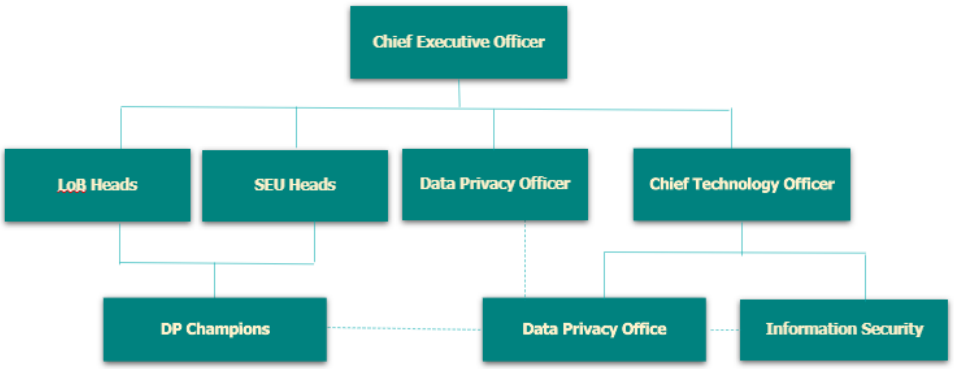
3.10 Data Privacy Risk Management

DP Office owns the Data Privacy risk governance in IBS.

Unit level Data Privacy risks are identified and managed by each unit. The Data Privacy Champion in each unit will lead the risk management. Risks that requires attention and intervention at an enterprise level will be tracked and managed by the DPO.

Risks requiring attention at an enterprise level will be reported to the Senior Leadership team as part of the DPO Reporting.

3.11 Data Privacy Organization



Data Protection Officer

IBS shall appoint a Data Protection Officer to inform and advise IBS and its employees about their obligations to comply with this Policy and the applicable data protection laws. Data Protection Officer with the help of data protection coordinators monitor the compliance of this Policy and applicable data protection laws, including managing internal data protection activities, advising on DPIA, conducting internal audits, and providing the required training to employees. The Data Protection Officer shall report to Chief Executive Officer of IBS. The role and responsibility of Data Protection Officer will be as per the General Data Protection Regulation (EU 2016/679).

Anyone who considers that there has been a breach of this Policy may make a complaint to Data Protection Office. The complaint will be reported to the Data Protection Officer who may be asked to advice on the response. All concerns and complaints will be handled confidentially. Inquiries by supervisory authorities must always be reported to the Data Protection Officer.

Contact details for the Data Protection Officer:

Saikumar Viswanathan
Data Protection Office,
E-mail: dataprotectionoffice@ibsplc.com

DPO Team

- Responsible for Data Privacy Compliance in IBS
- Works with Senior Leadership team to define privacy objectives
- Define Privacy Policy for the organization
- Manages Privacy Risk in IBS
- Establish and track the Privacy Strategy for each unit, aligned with the Privacy Policy
- Report Privacy Compliance, to the Senior Leadership team
- Monitor regulatory changes and perform enterprise level Privacy Impact Assessment
- Responsible for Personal Data Breach Handling and Privacy Request Handling

DP Champions

- Responsible for Data Privacy Compliance in the respective unit
- Define privacy strategy for the unit, with guidance from DPO team
- Lead privacy compliance of the unit, by implementing the privacy strategy
- Own the PII Inventory Lists of the unit
- Conduct Privacy Impact Assessment in the unit
- Monitor and report the compliance status to DPO team

4. References

- IBS Information Security Policy
- IBS Information Classification Policy
- IBS Data Loss Prevention Policy
- IBS Information Security Incident Management Policy
- IBS Logical Access Control Policy
- IBS E-mail Security Policy
- IBS Website Privacy Policy
- IBS Internet Security Policy

Appendix 1:Definitions

Data Controller shall mean any natural or legal person, public authority or agency which determines the purposes and means of Processing of Personal Data. For e.g. for the purpose of a contract with a customer, that customer shall be the Data Controller.

Data Subject means the natural person to whom Personal Data relates.

Employee Consent Form means the consent form expressly agreed by all employees, as part of the recruitment, on-boarding or employment process.

Personal Data shall mean the information that can be used on its own or with other information to identify, contact, or locate a natural person, or to identify an individual in context. e.g., Name, Address, Phone Number, IP Address etc.

Processing or to Process shall mean any operation that is performed on Personal Data, whether or not by automatic means, such as collection, recording, storage, organization, alteration, use, disclosure (including the granting of remote access), transmission or deletion of Personal Data.

Sensitive Personal Data shall mean Personal Data that reveal an individual's racial or ethnic origin, political opinions or membership in political parties or similar organizations, religious or philosophical beliefs, membership in a professional or trade organization or union, physical or mental health including any opinion thereof, disabilities, genetic code, addictions, sexual orientation, criminal offences, criminal records, proceedings with regard to criminal or unlawful behavior, or social security numbers issued by the government, or any other type of data that qualifies as Sensitive Personal Data under applicable local law.

Supplier shall mean any Third Party that provides goods or services to IBS (e.g. an agent, consultant, intermediary or vendor).

Staff shall mean all employees and other persons who Process Personal Data as part of their respective duties or responsibilities using IBS information technology systems or working primarily from IBS's premises.

Third Party shall mean any person, private organization or government body outside IBS.

Appendix 2: List of Designated Personnel

Data Subject may contact the following IBS designated personnel, for any updates or corrections to their Personal Data.

Role of Data Subject	IBS Designated Role
Employee	HR Business Partner
Vendor	Procurement Manager
Customers	Account Manager

History

Version	Date	Author	Remarks
0.1	04-Jun-2018	Manoj S V	Draft
0.2	05-Jun-2018	Manoj S V	Valid after incorporating review comments from Saikumar V
0.3	11-Jun-2018	Premanand SK	Incorporated review comments from Arun Hrishikesan
1.0	17-Sep-2018	Premanand SK	Approved by Arun Hrishikesan
2.0	8-Jun-2020	Premanand SK	Status remains Approved after updating to latest template format
2.1	16-Oct-2020	Premanand SK	Incorporated review comments
3.0	21-Oct-2020	Premanand SK	Approved by CTO