
PI010– PERSONAL DATA PROTECTION PRIVACY POLICY



Version History

Version No.	Release Date	Description Of Change	Prepared By	Reviewed By	Approved by
1.0	24-Aug-22	Initial Release	Manjiree Joshi	Mrudulini Ohol	Tanmoy Adak

TABLE OF CONTENTS

1	PURPOSE	4
2	SCOPE.....	4
3	RESPONSIBILITY.....	4
4	DOCUMENT AND RECORD REFERENCE.....	4
5	POLICY STATEMENT	5
6	POLICY GUIDELINES.....	5
7	DATA COLLECTION, PROCESSING AND TRANSFER.....	5
8	CONSENT.....	6
9	CONFIDENTIALITY AND SECURITY.....	6
10	DATA SUBJECT ACCESS, CORRECTION, DELETION AND PROTABILITY.....	7
11	PRIVACY BY DESIGN.....	7
12	DATA PROTECTION IMPACT ASSESSMENT.....	7
13	BREACH NOTIFICATION	8
14	DEFINITIONS.....	8

PERSONAL DATA PROTECTION PRIVACY POLICY

1 PURPOSE

To demonstrate a set of Privacy and Personal Data Protection standards that govern “Bitwise” procedures to collect, store and process Personal Data in a lawful manner.

- To provide consistent treatment of Personal Data throughout Bitwise entities
- To ensure Personal Data is protected from data security risks
- To ensure Personal Data is transferred or processed in a manner consistent with the applicable data protection laws and regulations.

2 SCOPE

- This policy shall apply to Bitwise, its operations and business units and supersedes any other policy relating to Personal Data protection. This means that this Policy shall apply to all employees, contractors, working partners and businesses carried on by Bitwise and any other Affiliates of Bitwise except to the extent, if any, stated under exemptions below, shall comply with it.
- This policy is applicable to all employees, contractors, and consultants of Bitwise at all locations or needs access to Bitwise Information processing facilities.
- The scope further includes all identified business and support processes of Bitwise Digital and its subsidiaries at all locations.

3 RESPONSIBILITY

All employees, contractors, and third-party vendors of Bitwise handling Personal Data shall take reasonable measures for protection of Personal Data. The Data Protection Officer (DPO) is responsible for administration of this policy and monitoring its compliance.

4 DOCUMENT AND RECORD REFERENCE

- General Data Protection Regulation (GDPR).
- ISO/IEC 27001:2013
- ISO/IEC 27701:2019

5 POLICY STATEMENT

'Bitwise shall ensure that Personal Data relating to natural persons including employees (current as well as former) suppliers, and customers, are obtained and processed fairly, and in accordance with the data subjects' rights under Data Protection Laws and Regulations. Bitwise respects the privacy and is committed to promoting the responsible use of personal information and protecting individual's privacy rights.

6 POLICY GUIDELINES

- 6.1 Bitwise shall as a data controller or processor, establish the specific purposes for which Personal Data is being collected and that its collection and processing of Personal Data is done in a manner consistent with those stated purposes.
- 6.2 Bitwise shall collect and process only such Personal Data as is adequate, relevant and limited in scope to the requirement and for a length of time that is necessary for the stated purposes of its use.
- 6.3 Bitwise shall utilize IT systems and applications that have the ability to comply with Data Protection Laws and Regulations including providing appropriate security for storage and transmission of Personal Data.
- 6.4 Bitwise shall Perform Data Protection Impact Assessments as per GDPR requirements.
- 6.5 Bitwise shall report breaches promptly and in line with the Personal Data breach notification process.
- 6.6 Bitwise shall record, investigate, analyse and report data protection-related complaints.
- 6.7 Bitwise shall ensure that data protection training is undertaken by all concerned employees.

7 DATA COLLECTION, PROCESSING AND TRANSFER

Bitwise may collect, store, use and disclose information about individuals which may constitute Personal Data (including Sensitive Personal Data) under various applicable data protection laws (including but not limited to Information Technology Act 2000 (IT Act), Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 (IT Rules), General Data Protection Regulation (GDPR), for lawful, explicit and legitimate purposes and for further processing of Personal Data consistent with those purposes.

The Personal Data may be processed for purposes including without limitation:

- Towards fulfilment of services offered including contractual obligations.
- Managing employee, vendor and client relationship.
- Operational purposes for human resource, recruitment, contract management for clients and vendors.
- Conducting market research.
- Providing individuals with information concerning products and services which Bitwise believes to be of interest.
- Compliance with any requirement of law, regulation, associations, codes that Bitwise decides to adopt.
- For the detection, investigation, monitoring and prevention of fraud and other crimes or malpractice.
- For the purpose of, or in connection with, any legal proceedings for obtaining legal advice or for establishing, exercising or defending legal rights or any other purpose connected to or incidental to the purposes stated above.

- Personal Data collected at website - cookies may be used in website to track user behaviour, etc., and/or username, address, email, phone number may be collected for marketing or research purposes. Any transfer of Personal Data to a third party shall take place only if, adequate levels of protection of Personal Data in accordance with applicable data protection laws is guaranteed by such third party. Data shall be encrypted and anonymized wherever necessary.

The employees/ stakeholders must not transfer/ share any personal data internally with other employees, members of any other department of Company, third party and outsiders unless instructed by their approving hierarchy or Data Protection Officer. Data Processing Addendums (“DPA”) or similar data transfer agreements should be executed when Company shares any Personal Data with any third party.

8 CONSENT

- Wherever personal data is collected, stored and processed Bitwise shall obtain consent from the data subject prior to collecting of personal data
- The consent shall be voluntary and revocable
- The consent shall be for the purpose being collected
- Records of all consent shall be maintained
- Process to handle revocation of consent shall be defined.

Bitwise shall specifically mention the purpose and obtain free consent from the data subject prior to collecting, storing and processing of Personal Data.

Bitwise shall not utilize an individual’s Personal Data in its control, beyond the scope for which it was collected without prior written consent from the individual. Individual’s Personal Data shall not be provided or otherwise disclosed to third parties other than Bitwise, investigators, or law enforcement personnel where consent has been obtained from the concerned individual or when disclosure is legally mandated.

Bitwise may record and monitor electronic and voice communications, to the extent permitted by applicable laws, to ensure compliance with the legal and regulatory obligations, internal policies and for the purposes outlined above in this policy.

9 CONFIDENTIALITY AND SECURITY

Bitwise shall take prudent steps to safeguard the confidentiality and security of all Personal Data including taking procedural and organizational steps to protect Personal Data from accidental or unlawful destruction and disclosure. These steps include entering into written agreements to protect Personal Data with all its vendors, subcontractors who process Personal Data.

In addition, Bitwise strives to protect personally identifiable information that it maintains or disseminates so that it is not accessed or obtained by unauthorized individuals or used in unauthorized ways.

10 DATA SUBJECT ACCESS, CORRECTION, DELETION AND PROBABILITY

Bitwise recognizes that data subjects have a right to request a copy of the Personal Data held by Bitwise. If any Personal Data is found to be incorrect, the individual concerned has the right to file a request to amend, update or delete it, as appropriate. Individuals also have a right to object to the processing of their Personal Data as per the prevailing laws.

If Bitwise undertakes transactions or other services that involves the processing or disclosure of Personal Data on behalf of any of our client or counterparty, it shall be the responsibility of such client or counterparty to ensure that it has all necessary authority to permit Bitwise to process and disclose the Personal Data accordingly.

Privacy consent can be withdrawn by the data subject by informing the appropriate authority within Bitwise as mentioned in Request Handling Procedure.

The personal data shall be deleted from the system on request or as per the Data Retention Policy, only after a complete evaluation of compliance with any applicable legal obligations or business processes.

Data Subjects shall be notified on action taken on the request of the individuals without any undue delay (within a timeframe as specified under the applicable laws) from receipt of request.

Sr. No	Location	Response Timelines
1	Europe Laws (GDPR)	30 days
2	UK Data Protection Laws	30 days

11 PRIVACY BY DESIGN

Privacy controls shall be considered while designing and implementing new or existing systems or processes, based on the technologies available, cost of implementation, scope, context and purposes of collecting, storing and processing Personal Data.

Bitwise shall implement appropriate data-protection principles, technical and organizational measures, such as pseudonymisation, data minimization, data encryption, etc. to ensure that Personal Data is secure.

12 DATA PROTECTION IMPACT ASSESSMENT

Bitwise shall conduct periodical Data Protection Impact Assessment that shall include:

- A systematic description of the system or purpose.
- Assessment of the risks to the rights and freedoms of data subjects.

- The measures to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data and to demonstrate.

13 BREACH NOTIFICATION

All Bitwise employees, contractors, and third-party vendors handling Personal Data have a responsibility to report any personal data breach related incidents and any violations of this policy and/or other data protection policies immediately to DPO@bitwiseglobal.com.

14 ENFORCEMENT

Enforcement of this Policy and its Annexures is mandatory and any violations of this policy and/or its Annexures should be reported through the Breach Handling Policy.

The steps to be taken in case of any violation by Bitwise and its Affiliates personnel:

- All violations shall be reported immediately to the Data Protection Officer (DPO) at DPO@bitwiseglobal.com .
- Any Bitwise personnel found violating this policy will face strict action taking into account factors such as nature of violation, degree of damage caused etc., and which may include termination or any other legal action.

15 DEFINITIONS

Bitwise shall mean and include its Affiliates and group entities.

Affiliates mean Bitwise and (a) any persons or entities that, now or in the future, directly or indirectly, control, are controlled by them, or are under common control, or (b) any persons or entities that are acquired, managed, or operated by them, whether by membership, stock ownership, joint operating agreement, or other substantial relationship.

Data Protection Laws and Regulations means, in the European Union, the Data Protection Directive 95/46/EC and the national statutory legislation passed in each Member State implementing this Directive, the General Data Protection Regulation (GDPR) 2016 / 679, United Kingdom GDPR, the United Kingdom Data Protection Act 2018, the Privacy and Electronic Communications Regulations as well as applicable data protection and privacy laws that exist outside the EU in each country.

European Union – means the current EU Member State countries of: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain and Sweden.

Personal Data under GDPR means any information relating to an identified or identifiable natural person ('data subject'); 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.

Personal information' under Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 (Privacy Rules) means any information that relates to a natural person, which either directly or indirectly, in combination with other information that is available or likely to be available to a corporate entity, is capable of identifying such person.

Processing 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, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Specified purpose means being clear from the outset about why we are collecting Personal Data and are transparent about our purposes with the individuals concerned.

Sensitive personal data or information under Privacy Rules—means such personal information which consists of information relating to;— (i) password; (ii) financial information such as Bank account or credit card or debit card or other payment instrument details ; (iii) physical, physiological and mental health condition; (iv) sexual orientation; (v) medical records and history; (vi) Biometric information; (vii) any detail relating to the above clauses as provided to body corporate for providing service; and (viii) any of the information received under above clauses by body corporate for processing, stored or processed under lawful contract or otherwise: provided that, any information that is freely available or accessible in public domain or furnished under the Right to Information Act, 2005 or any other law for the time being in force shall not be regarded as sensitive personal data or information for the purposes of these rules.