## 1.0 INFORMATION SECURITY POLICY

### 1.1. Overview

Adapty Solutions Pvt Ltd (herein referred to as Adapty) is committed to ensuring the Confidentiality, Integrity, and Availability (CIA) and provide comprehensive protection to its information assets againstthe consequences of confidentiality breaches, failures of integrity and/ or interruptions to their availability. Adapty will implement procedures and controls at all levels to protect the confidentiality and integrity of information stored and processed on its systems and ensure that information is available only to authorized persons as and when required.

This policy is to ensure the protection of its information assets, and to allow the use, access, and disclosure of such information in accordance with appropriate standards, laws, and regulations.

All workforce members, customers, and third parties who use Adapty' information processing facilities are required to comply with the Information Security policy of Adapty. All the existing Adapty' policies, related to personnel, administration, protection of confidential information, and other areas would apply equally to the information systems environment.

### 1.2 Objective

"Adapty committed to ensuring integrity, confidentiality, availability, and security of its physical and information assets at all times for serving the needs and expectations of its interested parties both within organization and from external parties including clients, suppliers, regulatory, and governmental departments in line with its vision, mission, and values while meeting all legal, statutory, regulatory, and contractual requirements. Adapty' information systems and the information and data they contain arefundamental for its daily operations and future success. Adapty will develop, implement, maintain, and continually improve policies, procedures, and controls at all levels to protect the confidentiality and integrity of information stored and processed on its systems and ensure that information is available to authorized persons as and when required."

### 2. Scope

Applicable to all full /Part time employees of Adapty

### 3. Responsibilities

- Concerned Employee/ Reporting Manager
- Corporate Security and Compliance / IT Team

## 4. Governance and Organization Structure

- Adapty has established a Corporate Security and Compliance Team (CSC) made up of key personnel whose responsibility is to identify areas of security and compliance concern acrossAdapty and act as the first line of defense in enhancing the appropriate security and compliance posture.
- The team comprises the workforce who are knowledgeable in legal cross-regulation, policy, products, and IT, and are interested in ensuring five of the trust principles—confidentiality, integrity, availability, privacy, and security—with regard to data protection by law, compliance, and standards across Adapty. The CEO has assigned the responsibilities and authority to Data Protection Officer for overseeing and maintaining information security and compliance as per the standard and industry best practices.
- The governance of these programs is performed by the Corporate Security and Compliance Committee, consisting of executives and other department heads from across Adapty.

### 4.1 Personnel Security

- Adapty has established a formal sanctions policy and process for personnel failing to comply with established information security and compliance policies and procedures.
- Adapty has established personnel security requirements, including security roles and responsibilities for third-party providers, and monitors provider compliance.
- Adapty screens individuals requiring access to critical and production environment information and information systems before authorizing access. The only workforce with the highest clearance has access to our data center. Workforce access is logged, and passwords are strictly regulated. We follow as need basis access principles to production data to only a selectfew of these workforces who need such access to provide support and troubleshooting.
- As per the established process, on termination of individual employment, Adapty terminates information system access, conducts exit interviews, retrieves all organizational information system-related property, and provides appropriate personnel with access to official records created by the terminated workforce that are stored on organizational information systems.
- Adapty has developed a world-class practice for managing security and data protection risk.
- Awareness and Training
    - All employee completes an annual information security and privacy awareness and training program.
    - As part of this program, additional role-based training is provided to the workforce, before they start handling sensitive and confidential information.
    - Information Security and Compliance Training Guide is provided as a quick referenceguide.
    - Training logs identifying the training class, attendee, and date are kept by the HR department.

### 4.2. Information Asset Management

- Adapty has established a formal Asset Management policy; and the process is necessary to facilitate effective management, control, and maintenance of the assets/information to its operations environment by classifying assets as per the functionality or criticality.

- This policy to identify, classify, label, and handle Information Assets of Adapty and to apply protection mechanisms commensurate with the level of confidentiality and sensitivity.
- The confidentiality and sensitivity of information will be maintained through an Information Asset classification scheme. The level of security to be accorded to the information of Adapty depends directly on the classification level of the asset, which is associated with that information.
- The Information Asset Inventory must contain the following information as a minimum:
    - Information Asset Identification
    - Information Asset Description
    - Information Asset Location
    - Information Asset Owner/Custodian
    - Information Asset Classification

### 4.3. Information at Adapty

Adapty information may include, but is not limited to:

- All proprietary information that belongs to Adapty such as user manuals, training materials, operating and support procedures, business continuity plans, and audittrails.
- Personnel information relating to employees of Adapty.
- All client information & product research-related data held by Adapty.
- All software assets such as application software, system software, development tools,and utilities.
- All physical assets, such as computer equipment, communications equipment, removable media, and equipment relating to facilities.
- People assets.
- Intangibles asset such as the reputation and image of Adapty.

### 4.4. Access Control

The access controls required to meet the security objectives of the Information Security policy. Accesscontrol management is paramount to protecting Adapty information resources and requires implementation of controls and continuous oversight to restrict access.

Confidentiality, Integrity, and Availability (CIA) are fundamental aspects of protection of systems and information, and are achieved through logical, physical, and procedural controls. It is vital for the protection of systems and information authorized users who have access to Adapty systems and information are aware of and understand how their actions may affect security and privacy.

The policy is organized into the following key sections:

- Business Requirements for Access Control
- User Access Management
- User Responsibilities
- Application and Application Access Control
- Mobile Computing and Teleworking

- Access control is established by imposing standards for protection at the operating system level, at the Application level, and at the Database level. Access to Adapty computer systemswill be based on the principles of “least privilege” and "need to know” and must be administered to ensure that appropriate level of access control is applied to users as well as system supportpersonnel to protect Adapty.
- All access to Adapty systems and services are reviewed by CSC and updated on a quarterly basis to assure proper authorizations are in place commensurate with job functions.
- Access to electronically stored records containing personal information will be electronically limited to those workforces having an authorized and unique login ID assigned.
- Where practical, all visitors are restricted from areas where files containing personal information are stored. Alternatively, visitors must be escorted or accompanied by an approved person inany area where files containing personal information are stored.
- Cleaning personnel (or others after normal business hours and not also authorized to have access to personal information) are not to have access to areas where files containing personalinformation are stored.
- All computers with an Internet connection or any computer that stores or processes personal information must have a recently updated version of software providing virus, anti-spyware, and anti-malware protection, installed and active at all times.
- Password Management: We have processes designed to enforce minimum password requirements for Adapty Service. We currently enforce the following requirements and security standards for end user passwords on Adapty Service:
    - Passwords must be a minimum of 8 characters in length and include a mix of uppercase and lowercase letters as well as numbers and symbols.
    - Multiple sign-ins with the wrong username or password will result in a locked account,which will be disabled for a period of time to help prevent a brute-force sign-in, but notlong enough to prevent legitimate users from being unable to use the application.
    - Email-based password reset links are sent only to a user's pre-registered email address with a temporary link.
    - Adapty prevents reuse of recently-used passwords.

### 4.5. Physical and Environmental Security

Our data centers are hosted in some of the most secure facilities available today in locations and useindustry best practices that are protected from physical and logical attacks as well as from natural disasters, such as earthquakes, fires, and floods. Physical security measures for these data centers include intrusion protection measures and security guards. We rely on third-party attestations of their physical security. Within our office premises, we employ a number of best industry-standard physical security controls.

## 5. Operational Security

- Adapty has established a formal policy and process for the requirements and key informationsecurity considerations for information technology operations, including the definition ofstandard operating procedures, change management, configuration management, release management, information backup, and restoration and cloud computing.

There are a number of controls in place to achieve the protection of data, information,and information system:

- Operational Procedure and Responsibilities
- Change Management
- Protection from Malware
- Information Backup
- Logging and Monitoring
- Operational Software Control
- Technical Vulnerability Management
- Information System Audit Control

- **Risk Management:**
  - Adapty is not willing to accept any risk that might damage customer trust. In addition,any risks that threaten to make us non-compliant to regulations and standard.
  - The possible values of existing risk acceptance/treatment/transfer level of residualrisk post calculation are:

| Slab Level | Risk rating | Risk Description | Management action |
|---|---|---|---|
| 1st | 1 | Negligible Risk | Accept risk - No actionrequired |
| 2nd | 2 | Low Risk | Accept risk - No action required |
| 3rd | 3 | Moderate Risk | Treat/ transfer risk |
| 4th | 4 | High Risk | Treat/ transfer risk |
| 5th | 5 | Very High risk | Treat/ transfer risk |

  - Risk Treatment Plan involves prioritizing, evaluating, and implementing appropriate controls as per the risk computation. A treatment plan shall be prepared for each identified risk as per the risk assessment performed where existing risk rating is greater than 2.

### 5.1. Communication Security

Adapty has deployed an information technology network to facilitate its business and make it more efficient for various risks. And establish management direction, principles, and standard requirement to ensure that the appropriate protection of information on its networks maintained and sustained. Few controls which in place to achieve the protection of exchanged information from interception, copying, modification, misrouting, and destruction as follow:

- **Network Controls**: Adapty monitors and updates its communication technologies periodicallywith the goal of providing network security as per industry best practices cryptographic techniques are used to protect the confidentiality, integrity, and authenticity of sensitive and confidential information. Firewall rules and access restrictions are reviewed for appropriateness on a regular basis.
- **Infrastructure Controls**: Adapty uses an Intrusion Detection System (IDS), a Security Incident Event Management (SIEM) system and other security monitoring tools on the production servers hosting

the Adapty product service. Notifications from these tools are sent to the Adapty Security Teamso that they can take appropriate action.

- **Secure Communication**: All data transmissions to Adapty services are encrypted using TLSprotocols, and we use certificates issued by SHA 256 based CA ensuring that our users havea secure connection from their browsers to our service. We use the latest and updated ciphersuites. Adapty Products are always communicated via HTTPS using Transport Layer Security(TLS), a cryptographic protocol that is designed to protect against eavesdropping, tampering,and message forgery.
- Adapty Product is always connected to the web-app via HTTPS using Secure Sockets Layer (SSL), a cryptographic protocol that is designed to protect against eavesdropping, tampering, and message forgery.
- Retention and disposal guidelines for all business correspondence including messages, in accordance with the defined standard.
- Segregation of the network shall be done by establishing V-LAN/ DMZ architecture. In either case, Testing, Production and Development environment shall be segregated as well.
- Agreements have been established for the secure transfer of business information to externalparties (such as customers, suppliers, and other interested parties).
- The roles and responsibilities for management of network security shall be clearly defined, communicated and reviewed on a regular basis to ensure optimum operative effectiveness and necessary segregation of duties shall be done to attain the said objective.

### 5.2. System Acquisition, Development, and Maintenance

Adapty has established Software Development Lifecycle adopted for planning, requirement analysis, design, development, testing and maintenance of the product Visual Website Optimizer (VWO) and PushCrew (PC). There are controls which in place to achieve the information security and data protection requirements as follow:

**Product Security**

- Adapty product security practices are measured using industry standard and methodologies security models. Adapty follows Agile methodologies for feature delivery and Scrum is used for new feature delivery. The SDLC for the Adapty Product services includes many activities to enhance security and privacy posture:
    - Defining security and privacy requirements
    - Design (threat modeling and analysis, security design review)
    - Development controls (static analysis, manual peer code review)
    - Testing (dynamic analysis, 3rd party security vulnerability assessments and Pen Test)
- Adapty Product designs, reviews, and tests the software using applicable OWASP and CISstandards.
- We use Definition of Done (DoD) to maintain the quality of deliverables, a clear and consistent Definition of Done is an effort to create an objective framework for quality. DoD provides a clear guideline to the team and to the stakeholders around exactly what needs to be done for eachStory, Sprint, Release, and Task to ensure a consistent and sustainable quality of deliverables. It ensures transparency and quality fit for the purpose of the product and organization

**Code Security**

- Adapty Product code is stored in a Stash / Atlassian system hosted by most secure data centers facilities. Adapty adopts a strict, least access privileges principle for providing access to the code. Commits to production code are strictly reviewed, and approval is restricted to just two people (Chief Technical Officer and Lead Engineer), after passing Unit Testing and QA in Testand Staging.
- Manual source code analysis on security-sensitive areas of code.
- The Adapty development team is trained on Open Web Security Application Project (OWASP) Secure Coding Practices and uses industry best practices for building secure apps.

**Bugs Reporting**

Adapty takes the security of its systems seriously and values the security community. The responsible disclosure of security and privacy vulnerabilities helps Adapty in ensuring the security and privacy of its users. Bugs can be reported through email at ithelpdesk@adapty.com.

### 5.3. Third-Party Supplier

- Adapty provides essential services and business functions which rely on IT solutions and applications contracted by third-party suppliers, which may be primary or subcontractors.
- Adapty maintains the integrity and accuracy of its information to meet its goals and obligations, both to the business and to people. To ensure this, it is essential that information is secured in line with professional best practices as well as statutory, regulatory, and contractual requirements that maintain confidentiality, integrity, and availability of all information assets.
- Adapty has established a formal Third-Party Supplier policy and put in place a procurement process so that contracts and dealings between Adapty and third-party suppliers have acceptable levels of data protection and information security in place to protect information (such as personal & company data) and maintain the confidentiality, availability, and integrity of information and are fit for purpose. Information security requirement will vary according to the type of contractual relationship with each supplier. There are a few controls in place to achieve protection of data, information, and information system as follows:
    i. Information security and controls should be formally documented in a contractual agreement which may be part of or an addendum to the main commercial service contract.
    ii. Separate Non-Disclosure Agreement should be used where a more specific level of control over confidentiality is required.
    iii. Appropriate due diligence must be exercised in the selection and approval of new supplier before the contract is agreed.
    iv. The information security provisions in place at existing suppliers (where due diligencewas not undertaken as part of initial selection) must be clearly understood and improved where necessary.

v. Access to Adapty, information should be limited wherever possible according to clear business needs.
vi. Basic information security principles such as least privilege, separation of duties, anddefense in depth should be applied.
vii. Adapty will have the Rights to Audit the information security and privacy practices ofthe supplier and/or the subcontractor.
viii. Supplier access to Adapty information resources is granted solely for the work contracted and for no other purpose.
ix. The supplier must comply with all applicable data protection regulation, best practice standards, and agreements.
x. On termination of a supplier or supplier employee from the contract for any reason, the supplier will ensure that all sensitive and confidential information is collected and returned to Adapty or destroyed within 24 hours.

- The security of information is fundamental to Adapty' compliance with data protection legislation and a key focus in its risk assessment, procurement, and management strategy.

### 5.4. Due Diligence

Before contracting with a third-party supplier, it is incumbent upon Adapty to exercise due diligence in reaching as much understanding as possible of the information security approach and controls the company has in place. It is important that the documented "supplier due to diligence assessment" procedure is followed so that all the required information is collected and an informed assessment can be made.

### 5.5. Contract

All Adapty contracts will clearly define each party's data protection and information security responsibilities toward the other by detailing the parties to the contract, effective date, functions or services being provided (such as defined service levels), liabilities, limitations on use of subcontractors and other commercial/legal matters normal to any contract.

The processing must be governed by a contract in writing between the controller and the processor, setting out the following:

- Subject matter and duration of the processing
- Nature and purpose of the processing
- Type of personal data and categories of data subjects involved
- Obligations and rights of the controller and processor

### 5.6. Reporting Security and Privacy Breaches

- Adapty has a Security Incident Response Plan designed to promptly and systematically respond to security, privacy, and availability incidents that may arise. The incident response plan is tested and refined on a regular basis.
- The primary focus of the plan is detecting, analyzing, prioritizing, and handling security incidents.
- Adapty follows policies and procedures to detect, respond to, and otherwise address security incidents including procedures to:
    - Identify and respond to suspected or known security incidents followed by mitigatingtheir harmful effects and documenting these incidents along with their outcomes.
    - Restore the availability or access to Customer Personnel.
    - Retrieve data in a timely manner.
- Notice: Adapty agrees to provide a prompt written notice within the time frame required under Applicable Data Protection Law(s) to a customer's Designated POC if it knows or suspects thata security incident has taken place. Such notice will include all available details required under Applicable Data Protection Law(s) for the customer to comply with its own notification obligations to regulatory authorities or individuals affected by the security incident.
- Under no circumstances should a user attempt to resolve any security and privacy breach on their own without first consulting the Adapty DPO. Users may attempt to resolve security and privacy breaches only under the instruction of, and with the express permission of the DPO.

### 5.7. Business Contingency and Disaster Recovery

Adapty has established a formal business contingency management (BCM) plan and a Disaster Recovery Plan (DRP) to minimize downtime of the critical business process, and recovery within required and agreed business timescales in the event of a disaster. Adapty has also created a clearly defined framework for the ongoing management of the BCM activities and provide guidelines for the development, testing, maintenance, and implementation of business continuity plans.

- Adapty defined two categories of systems from the disaster recovery perspective:
    - **Critical Systems**: These systems host application servers and database servers or are required for the functioning of systems that host application servers and database servers. These systems, if unavailable, affect the availability of data and must be restored, or have a backup process to restore these, immediately on becoming unavailable.
    - **Non-Critical Systems**: These systems include the ones that are not considered most critical. These systems, while they may affect the performance and overall security of critical systems, do not prevent critical systems from functioning and being accessed appropriately. These systems are restored at a lower priority than critical systems.
- Backup: To prevent data loss due to human error, our application databases are backed upevery hour in an automated fashion.

- Data Replication: Our customer and application databases are timely replicated on backupservers along with our CDN servers which are geo-redundant.
- Internet Redundancy: Adapty is connected through multiple Tier-1 ISPs. So, if anyone fails or experiences a delay, you can still reliably get to your applications and information.
- DRP is tested on a half-yearly basis; and the results are documented, and revisions aremade, as necessary.

### 5.8. Compliance

- Adapty has established a formal Compliance Policy and Procedure which addresses aspects of compliance required to be adhered to and fulfilled with respect to Adapty' Information Security Policies. This policy also addresses the legal and compliance requirements pertaining to relevant statutory legislation, and contractual and regulatory obligations which Adapty is supposed to adhere to in order to protect its documents, records, and assets, thereby preventing the misuse of information processing facilities. Such efforts would help Adapty establish, maintain, and sustain the desired information security and privacy posture aligned with the Adapty strategic business plan, based on the best practices, standards, and principles.
- Adapty is committed to and conducts its business activities lawfully and in a manner that is consistent with its compliance obligations. The Legal and Regulatory Compliance (Compliance Policy) establishes the overarching principles and commitment to action for Adapty with respect to achieving compliance by:
    - Identifying a clear compliance framework within which Adapty operates.
    - Promoting a consistent, rigorous, and comprehensive approach to compliance throughout Adapty.
    - Developing and maintaining practices that facilitate and monitor compliance within Adapty.
    - Seeking to ensure standards of good corporate governance, ethics, and community expectations.
    - Engendering a culture of compliance where every person within Adapty accepts personal responsibility for compliance, and acts ethically and with integrity.
- Adapty has been identifying all relevant regulatory and legislative requirements as per its contractual requirements and organization's operational requirements and defining, documenting, and updating it on a regular basis.
- All records, as mandated by statutory/legal/regulatory authorities in India or of foreign origin, for which Adapty is responsible for compliance, will be protected from intentional or unintentional damage through natural causes.
- The retention limit of statutory records will be as mandated by the applicable legislation. However, for business records/documents, the business group heads and or HODs shall determine the retention limit with justification.
- Adapty will always seek to protect the privacy of the personal information of its customers, employees, and third parties with whom Adapty has signed the third-party agreement. Divulging of facts will be done only in keeping with statutory/contractual/regulatory/legal requirements. Such information will always be protected from getting misused, leaked, or falsified or traded with any interested party knowingly or unknowingly.

- Where logs are required to be maintained as per contractual/regulatory/statutory/legal requirement, these will be maintained for a specified duration.
- Data or records that are no longer required for business, legal, and/or regulatory purpose will be disposed of securely.
- Legal restrictions on the use of assets in respect of which there are IPRs (such as copyright, software license, trademarks, design rights, and others) will be complied with.
- Intellectual Property Rights of software programs, documentation and other information generated by or provided by Adapty users, consultants, and contractors for the benefit of Adapty, will be the property of Adapty.
- Intellectual Property Rights will be included in all contracts.
- Relevant statutory, regulatory, and contractual requirements for Adapty' information assets will be defined explicitly. Such requirements will include, but are not limited to:
    - Information Technology Laws (IT Act 2008/2011 Amended)
    - Software Licensing Requirements
    - Intellectual Property Rights (IPR) Laws
    - Labor and General Employment Laws
    - Health and Safety Laws
    - Environmental Laws
- As part of the information security audits by independent consultants or body, the appropriate confidentiality and non-disclosure agreements will be signed with them. And any access granted to the external shall be restricted immediately after completion of the audit.
- Compliance requirements are used to enforce a minimum level of security and privacy within Adapty. These are by no means a "finish line" for security and privacy.
- Information Security Program: Adapty agrees to implement appropriate technical and organizational measures designed to protect Customer Personal Data, Employee and third- parties' data, as required by the Applicable Data Protection Law(s). Further, Adapty agrees to regularly test, assess, and evaluate the effectiveness of its Information Security Program to ensure the security of the Processing. Adapty has comprehensive privacy and security assessments and certifications performed by regulatory or third parties.
- Any workforce member found to have violated this policy may be subject to disciplinary and/or legal action according to the Sanction policy.

Any security breach could lead to the possible loss of confidentiality, integrity and availability of personal or other confidential data like code and company's documents. The loss or breach of confidentiality of company and personal data is an infringement of the General Data Protection Regulation, contravenes Adapty's Data Protection Policy, and may result in criminal or civil action against Adapty.

The loss or breach of confidentiality of contractually assured information may result in the loss of business, financial penalties or criminal or civil action against Adapty. Therefore, it is crucial that all users of Adapty adhere to the Information Security Policy. Any security beach will lead to disciplinary action against the user.

**The General Data Protection Regulation (GDPR)-**It is a new piece of legislation which replaces the current data protection laws in the European Union. The GDPR gives individuals greater control over their personal data by setting out additional and more clearly defined rights for individuals whose personal data is collected and processed by organizations. The GDPR also imposes corresponding and greatly increased obligations on organizations that collect this data.

Personal data is any information that can identify an individual person. This includes a name, an IDnumber, a postal address, online browsing history, images or anything relating to the physical, physiological, genetic, mental, economic, cultural or social identity of a person.

The GDPR is based on the core principles of data protection which exist under the current law. Theseprinciples require organizations and businesses to:

- Collect no more data than is necessary from an individual for the purpose for which it will beused;
- Obtain personal data fairly from the individual by giving them notice of the collection and its specific purpose;
- Retain the data for no longer than is necessary for that specified purpose;
- To keep data safe and secure; and
- Provide an individual with a copy of his or her personal data if they request it.

**Under the GDPR individuals have the significantly strengthened rights to:**

- Obtain details about how their data is processed by an organization or business;
- Obtain copies of personal data that an organization holds on them;
- Have incorrect or incomplete data corrected;
- Have their data erased by an organization, where, for example, the organization has no legitimate reason for retaining the data;
- Obtain their data from an organization and to havethat data transmitted to another organization (Data Portability);
- Object to the processing of their data by an organization in certain circumstances;
- Not to be subject to (with some exceptions) automated decision making, including profiling.

**Payment Card Industry Data Security Standard (PCI DSS)**

The Payment Card Industry Data Security Standard (PCI DSS) Program is a mandated set of securitystandards that were created by the major credit card companies to offer merchants and service providers a complete, unified approach to safeguarding credit cardholder information for all credit card brands. In September of 2006, a group of five leading payment brands including American Express, Discover Financial Services, JCB, MasterCard Worldwide and Visa International jointly announced formation of the PCI Security Standards Council, an independent council established to manage ongoing evolution of the PCI standard. Concurrent with the announcement, the council released version
1.1 of the PCI standard. The PCI Data Security Standard requirements apply to all payment card network members, merchants and service providers that store, process or transmit cardholder data. The requirements apply to all methods of credit card processing, from manual to computerized; the most comprehensive and demanding of which apply to e-commerce websites, and retail POS systemsthat process credit cards over the internet.

**The Health Insurance Portability and Accountability Act (HIPPA**) – This sets the standard for protecting sensitive patient data. Any company that deals with protected health information (PHI) mustensure that all the required physical, network, and process security measures are in place and followed. This includes covered entities (CE), anyone who provides treatment, payment and operations in healthcare, and business associates (BA), anyone with access to patient information and provides support in treatment, payment or operations. Subcontractors, or business associates of business associates, must also be in compliance.

The HIPAA Privacy Rule addresses the saving, accessing and sharing of medical and personal information of any individual, while the HIPAA Security Rule more specifically outlines national security standards to protect health data created, received, maintained or transmitted electronically, also known as electronic protected health information (ePHI).
If you are hosting your data with a HIPAA compliant hosting provider, they must have certain administrative, physical and technical safeguards in place, according to the U.S. Department of Healthand Human Services. The physical and technical safeguards are most relevant to services provided byyour HIPAA compliant host as listed below, with detail on what constitutes a HIPAA compliant data center.
Physical safeguards include limited facility access and control, with authorized access in place. All covered entities, or companies that must be HIPAA compliant, must have policies about use and access to workstations and electronic media. This includes transferring, removing, disposing and re-using electronic media

6. **Grievance Officer -** Mr. Amol Potphode is appointed as a Grievance officer with effect of **22nd February, 2021.**

   **Contact Details**:
   **Mr. Amol Potphode**
   Adapty Solutions Pvt Ltd.,
   2nd Floor, Plot A-38, Rd Number 11,
   Wagle Industrial Estate, Thane West,
   Thane, Maharashtra 400604
   Email ID - **amol.potphode@adapty.com**
   Contact Number - **9930733474**

7. **Exception to Information Security Policy**

All the exceptions to the above policy can only be made / reviewed / appended with the dueapproval of the company's management.