GoodTech Pvt.

DATA PROTECTION POLICY

Document version: 1.1

Date: October 01,2023

GDPR and Data Protection Act 2018 Requirements

1 Version Control

	Last Modified	Last Modified By	Document Changes
1.0	02.01.2022	Anil (Information Security Officer)	Add new policies.

2 Table of Contents

1 Version Control 2
2 Table of Contents 3
3 Introduction 5
4 Data Protection Policy 6
4.1 Purpose 6
4.2 Scope 6
4.3 Principle 6
4.4 Definitions 6
4.5 Data Protection Policy Statement 7
4.6 Data Protection Framework 7
5 Legal Basis for Processing 8
6 Data Protection Principles 8
6.1 Lawfulness, Fairness and Transparency 8
6.2 Purpose Limitation 8
6.3 Data Minimization 9
6.4 Accuracy 9
6.5 Storage Period Limitation 9
7 Personal Information Classification and Handling 10
8 Personal Information Retention 10
9 Personal Information Transfer 10
10 Personal Information Storage 10
11 Breach 11
12 The Rights of Data Subjects 11
12.1 The right to be informed. 11
12.2 The right of access 11
12.3 The right to rectification 12
12.4 The right to erasure 12
12.5 The right to restrict processing. 12
12.6 The right to data Portability 12
12.7 The right to object 13

12.8 Rights in relation to automated decision making and profiling. 13
13 Data Definitions 13
13.1 Personal Data 13
13.2 Sensitive Personal Data 13
13.3 Data Controller 14
13.4 Data Processor 14
13.5 Processing 14
13.6 Anonymization 15
14 Policy Compliance 15
14.1 Compliance Measurement 15
14.2 Exceptions 15
14.3 Non-Compliance 15
14.4 Continual Improvement 16
14.5 Compliance with ISO 27001 16
15 Awareness and Training 16
16 Monitoring and Auditing 16
17. Policy Review and Revision 17
18 Conclusion 18

3 Introduction

As the Information Security Officer, introducing and presenting our Data Protection Policy is a tremendous honor and responsibility that I hold in the highest regard. This policy is not simply a collection of directives; rather, it serves as a stronghold of safeguards, built upon established norms and best practices in the industry. It has been carefully customized to conform to the rigorous criteria outlined in ISO 27001 standards.

Our steadfast dedication to protecting the privacy, availability, and integrity of our data assets serves as the foundation of this policy. These principles are not mere abstract notions; rather, they serve as the foundational pillars that support the meticulous construction of our organization's information security architecture. It is acknowledged that while the advent of the digital age has brought about unparalleled innovation and connectivity, it has also introduced an array of challenges and dangers that have not been witnessed before. The importance of safeguarding data and maintaining privacy has never been greater.

This policy represents more than just a declaration; it represents a serious dedication to safeguarding our sensitive data against the continuous and unrelenting onslaught of cyber threats. Our dedication transcends mere digital data bytes and bits; it also includes safeguarding intellectual property, financial records, customer information, and operational protocols. Their protection serves as the cornerstone upon which our organization's reputation and trust are constructed; these assets are vital to its operation.

Privacy has transitioned from being an indulgence to a fundamental entitlement and a legal requirement. Maintaining the confidentiality of our stakeholders' privacy is not merely an obligation; it is a moral necessity. In addition to adhering to legal and regulatory obligations, most notably the General Data Protection Regulation (GDPR), our Data Protection Policy guarantees that we exceed all reasonable measures to protect personal data and uphold the rights of individuals with regard to their personal information.

In my capacity as the Information Security Officer, I maintain an unwavering commitment to transforming this policy from a mere conceptual framework into an operational, practical document. My goal is to establish an organizational culture that prioritizes data protection, wherein each member of staff is cognizant of their responsibility to maintain the confidentiality and privacy of data. Our dedication to safeguarding data is not a one-time event; rather, it is a continuous process that necessitates ongoing education, vigilance, and adjustment in response to emergent risks and regulatory changes.

In an era where information is both the most valuable asset and the most susceptible target, protecting it is an absolute necessity and not a matter of choice. We remain steadfast in our commitment to surpassing industry standards as we commence this intellectual property safeguarding endeavor. Our dedication to ensuring the security of our data assets, safeguarding the privacy of our stakeholders, and serving as an exemplar of data protection excellence is reflected in our Data Protection Policy. As a collective, we shall uphold the confidence of our stakeholders and illustrate that safeguarding data is not merely an obligation, but rather a fundamental tenet of our corporate ethos.

4 Data Protection Policy

4.1 Purpose

The principal objective of this policy is to guarantee the organization's rigorous compliance with the legal and regulatory provisions delineated in the Data Protection Act 2018 and the General Data Protection Regulation (GDPR). This entails safeguarding the rights of data subjects, which comprise the foundational tenets of data privacy and the secure management of personal data. Through strict adherence to these stipulations, our policy aims to strengthen data protection, reduce potential hazards, and ensure the lawful and ethical handling of data assets.

4.2 Scope

This policy is applicable to all personnel affiliated with our organization, including contractors, third-party collaborators, and employees. Its extent is exhaustive. Furthermore, it encompasses all information systems and technologies that fall under our jurisdiction, guaranteeing the maintenance of consistent and secure data management across a wide range of platforms. The scope of this inclusiveness transcends data type and format constraints, encompassing a wide array of information regardless of its physical or digital storage format (e.g., hard copies, documents, servers). Our organization is fully dedicated to safeguarding data in every domain, ensuring that it is protected in a comprehensive and consistent manner.

4.3 Principle

The designation of personal information as "Confidential" in accordance with our data protection framework denotes its paramount importance. The categorization requires the rigorous implementation of corresponding policies, controls, and procedures that are specifically engineered to enhance the confidentiality and integrity of this information. Strict data management procedures, encryption, and secure storage are a few of the measures implemented. Through the designation of personal data at this level of classification, we emphasize our steadfast dedication to safeguarding sensitive information and maintaining the utmost levels of data security and privacy.

4.4 Definitions

- Data Assets: Any information collected, processed, stored, or transmitted by our organization, irrespective of format or location.
- The procedure of classifying data according to its level of sensitivity and significance.
- Data privacy refers to the safeguarding of personal information and the entitlements of individuals with regard to such data.

- Data security comprises the safeguards that are put in place to prevent unauthorized access, disclosure, modification, or deletion of data.
- A data breach occurs when an unauthorized individual gains access to, obtains, discloses, or loses data.
- The General Data Protection Regulation (GDPR) is a regulation of the European Union that safeguards the privacy and personal information of individuals.

4.5 Data Protection Policy Statement

Our organization, within the framework of our operational processes governed by the prevailing UK Data Protection Act 2018, carries the distinct roles of both a Data Controller and a Data Processor. This dual categorization reflects our unwavering commitment to safeguarding the privacy of personal information entrusted to us by our customers, clients, employees, and other stakeholders.

This Data Protection Policy serves as a resolute affirmation of our dedication to upholding the highest standards of data protection. In pursuit of this commitment, we have embarked on a comprehensive Information Security Management program meticulously aligned with the internationally recognized standard ISO27001. This strategic alignment ensures that the processing of personal information adheres to globally acclaimed best practices.

Our multifaceted role as both a Data Controller and a Data Processor underscores the complexity of our data protection obligations. As a Data Controller, we bear the responsibility for determining the purposes and methods of personal data processing. Simultaneously, as a Data Processor, we are entrusted with the secure and compliant processing of personal data on behalf of others. This demands a proactive and holistic approach to data protection that our organization diligently upholds.

By aligning with ISO27001, we affirm our unwavering commitment to data security, encompassing critical facets such as risk management, access control, and incident response. This program serves as a steadfast assurance that our processes for handling personal information are fortified with the highest levels of security and comply with globally recognized standards, thus establishing a robust foundation for data protection across our organization.

4.6 Data Protection Framework

Our Data Protection Policy is founded upon well-established industry standards and best practices, with an explicit emphasis on ISO 27001 compliance. By implementing this framework, we not only ensure that our data protection efforts are in line with the standards set by the industry, but we also elevate them to the utmost levels of data security and privacy. ISO 27001, an internationally recognized standard, reinforces our dedication to strengthening our data protection protocols, guaranteeing that our operations are thoroughly evaluated and upheld to the highest levels of security and privacy criteria.

5 Legal Basis for Processing

Our organization ensures that the legal basis for processing Personal Data is thoroughly determined and recorded in our comprehensive Record of Processing Activities, in compliance with Article 6 of the General Data Protection Regulation (GDPR), which specified the legal grounds for such processing. This documentation functions as an essential repository of the rationales that support our data processing operations, guaranteeing that we adhere strictly to legal requirements. By bolstering transparency and securing our dedication to the lawful and ethical management of Personal Data, it serves as an essential point of reference for internal and external stakeholders, showcasing our commitment to the regulatory framework established by the GDPR.

6 Data Protection Principles

Our organization upholds an unwavering dedication to handling data in strict adherence to its responsibilities as stipulated in the Data Protection Act 2018 and the General Data Protection Regulation (GDPR). Personal data are required to adhere to the principles of lawfulness, impartiality, and transparency, as stated in Article 5 of the GDPR. Additionally, it stipulates that data collection must be for legitimate, specific, and unambiguous purposes, restricted to what is essential, precise, current, and retained solely for the required duration. These principles synergistically strengthen our commitment to maintaining the confidentiality and lawfulness of personal data processing.

6.1 Lawfulness, Fairness and Transparency

- The data was lawfully, equitably, and transparently processed with respect to the individuals involved.

The data that we control and/or process has been reviewed and documented, and the legal basis for processing has been established. We furnish privacy notices that apprise data subjects of their rights, in addition to specifying the nature, entity, duration, and rationale of the processing that occurs.

6.2 Purpose Limitation

- Data collected for specific, legitimate, and explicit purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes shall not compromise the original purposes; and data shall be collected for legitimate, explicit, and specified purposes.

We guarantee that data is processed solely for the intended purposes for which it was collected and disclosed, and not for any other purpose without the consent and awareness of the data subject.

6.3 Data Minimization

- Sufficient, pertinent, and restricted to the bare minimum required for the objectives for which they are being processed.

We ensure that the data collected is suitable for the intended purpose and is not excessive. Data privacy impact assessments are performed throughout the course of our projects.

6.4 Accuracy

- Precise and, when required, current; each reasonable measure should be implemented to guarantee that personal data that is inaccurate in relation to the intended uses for which they are processed are promptly removed or corrected.

We ensure that data is routinely reviewed and evaluated for accuracy and have established procedures to promptly rectify and delete any errors that may occur.

6.5 Storage Period Limitation

- Maintained in a manner that enables the identification of data subjects for the shortest duration required for the intended purposes of processing the personal data. Personal data may be retained for extended durations, but only if the processing is for archival purposes, scientific or historical research, or statistical purposes, or subject to the implementation of the requisite technical and organizational safeguards mandated by the GDPR in that regard.

A data retention policy and schedule have been established in accordance with legal, regulatory, and organizational requirements.

- Processed using suitable technical or organizational measures to ensure the appropriate security of personal data, including protection against unauthorized or illicit processing and inadvertent loss, destruction, or damage.

An information security management system has been established in accordance with ISO 27001, which is the International Standard for Information Security. Throughout the life cycle of each project, we evaluate security controls and requirements in accordance with our information security culture.

7 Personal Information Classification and Handling

The classification and management of personal data adhere to the Information Classification and Handling Policy.

- A classification system will be implemented to assess the sensitivity, criticality, and impact of every data asset.
- On the basis of classification, access controls, data encryption, and data obfuscation techniques will be implemented.
- Protocols for the management of data will be implemented to guarantee the secure transmission and processing of information.

8 Personal Information Retention

Our Data Retention Schedule, Information Classification and Handling Policy, and Asset Management Policy are rigorously followed with regard to the retention and disposal of personal data. These regulating documents ensure that personal information is handled in accordance with its relevance and sensitivity. The duration for which data is retained is determined by the Data Retention Schedule. Upon its expiration, data is destroyed in a secure and irreversible manner, ensuring the protection of data subjects' privacy and rights in accordance with established best practices.

9 Personal Information Transfer

Personal data is transferred in strict adherence to our Information Transfer Policy. Employees assume a critical responsibility in upholding the prescribed level of security during the data transfer procedure, as delineated in the organization's policies and procedures. This ensures that personal information is transmitted in a secure manner, in accordance with established protocols and controls, thereby preventing unauthorized access or breaches and upholding the policy and industry standards requiring the protection of such data.

10 Personal Information Storage

Our Information Classification and Handling Policy is strictly followed when it comes to the storage of personal information. This policy guarantees that data is appropriately categorized and managed based on its level of sensitivity. Our Physical and Environmental Security Policy ensures that the storage environments are equipped with surveillance and access controls, among other precautions. The Cryptographic Control and Encryption Policy implements strong encryption protocols to safeguard electronically stored data. The backup policy guarantees data recovery and redundancy capabilities. In

addition, the Data Retention Schedule establishes the time limit for which personal information is retained and guarantees its secure disposal, thereby promoting data security and adherence to established norms.

11 Breach

When an incident occurs that violates the principles specified in the Data Protection Act 2018, it is the responsibility of our personnel to expeditiously notify their line manager, a member of the Management Review Team, and/or Senior Management. Concurrently, our established Incident Management Process is initiated in order to guarantee a coordinated and timely response. Instances of breaches are subject to a comprehensive evaluation, and prompt notification is provided to the affected data subjects and/or the Information Commissioner's Office, if deemed necessary. This proactive and transparent strategy is consistent with our dedication to safeguarding data, promptly mitigating potential risks, and adhering to legal and regulatory responsibilities.

12 The Rights of Data Subjects

12.1 The right to be informed.

It is within the rights of individuals to be apprised regarding the manner in which their personal data is utilized.

- The name and contact information of the organization in question.
- If applicable, the name and contact information of our representative.
- The contact information, if applicable, of our data protection officer.
- The intents behind the processing.
- The legal justification for the processing.

12.2 The right of access

- The right of individuals to access their personal data is inherent.
- This concept is frequently denoted as "subject access."
- Subjects have the ability to submit requests for access either orally or in writing.
- One month is allotted for our response to a request.
- It is generally not possible to impose a charge for processing a request.

12.3 The right to rectification

- Individuals have the right to have inaccurate personal data corrected or, if such data is insufficient, to have it completed, per the GDPR.
- An individual may submit a written or verbal request for rectification.
- One calendar month is allotted for the response of a request.
- There are specific situations in which a request for rectification may be denied.

12.4 The right to erasure

- The GDPR grants individuals the right to request the erasure of their personal data.
- "The right to be forgotten" is an alternative name for "the right to erasure."
- Erasure requests may be submitted either orally or in writing.
- One month is allotted for our response to a request.
- The privilege is not universal and is contingent upon specific conditions.
- Beyond this, the GDPR imposes an obligation on us to contemplate the deletion of personal data in additional ways.

12.5 The right to restrict processing.

- While individuals possess the right to request the restriction or erasure of their personal data, this right is not absolute and is applicable solely under specific conditions.
- We are permitted to store personal information under restricted processing conditions, but not to utilize it.
- An individual may submit a written or verbal request for restriction.
- One calendar month is allotted for the response of a request.

12.6 The right to data Portability

- The right to data portability grants individuals the ability to acquire and repurpose their personal data across various services for their own purposes.
- It enables them to securely and conveniently relocate, duplicate, or transfer personal information between IT environments without compromising its functionality.
- By doing so, individuals can avail themselves of applications and services that utilize this information to assist them in comprehending their spending patterns or locating superior deals.
- The privilege is restricted to data that a user has voluntarily disclosed to a controller.

12.7 The right to object

- Under specific conditions, the GDPR grants individuals the right to object to the processing of their personal data.
- It is against the law to prevent the use of an individual's information for direct marketing purposes.
- In additional situations where the right to object is applicable, we might be permitted to proceed with the processing if we can provide a compelling justification for doing so.
- Individuals must be informed of their right to object.
- An objection may be presented either orally or in writing.

12.8 Rights in relation to automated decision making and profiling.

In certain circumstances, individuals are entitled to opt out of being subjected to a decision if:

- It is rendered through automated processing.
- It has a legal ramification or a similarly substantial impact on them.

13 Data Definitions

13.1 Personal Data

"Data Subject" refers to any natural person whose data, whether directly or indirectly, can be ascribed to them through the utilization of an identifier. These identifiers encompass a diverse range, including but not limited to their name, identification number, location data, online identifier, or specific factors that are unique to their physical, physiological, genetic, mental, economic, cultural, or social identity. In essence, it encompasses any information that, when applied, can lead to the identification of an individual, highlighting the comprehensive scope of personal data and the vital need to protect such information in line with stringent data protection principles and regulations.

13.2 Sensitive Personal Data

Personal Data that is inherently sensitive and holds the potential to significantly impact fundamental rights and freedoms warrants particular protection. This heightened need for protection arises from the fact that the processing of such Sensitive Personal Data could entail substantial risks to the core principles of privacy and personal freedom.

Sensitive Personal Data encompasses a broad range of information, including but not limited to data that discloses racial or ethnic origin, political opinions, religious or philosophical beliefs, or membership in trade unions. It extends to genetic data and biometric data collected for the unique identification of individuals, as well as data pertaining to an individual's health, their sex life, or sexual orientation. The

sensitivity of this data mandates stringent safeguards to ensure its confidentiality, integrity, and secure handling, as even a minor breach could have profound implications for an individual's fundamental rights and freedoms. Consequently, it is imperative that such data is subjected to specific protection measures to mitigate risks and uphold the privacy and dignity of individuals.

13.3 Data Controller

A "Data Controller" refers to an individual or entity, which can be a natural person, legal entity, public authority, agency, or any other organizational body. In this capacity, the Data Controller assumes the responsibility of, either independently or in collaboration with others, establishing both the objectives and methodologies of processing Personal Data. They play a pivotal role in defining the reasons for data collection and the manner in which the data is processed, effectively exercising authority over the fundamental decisions surrounding Personal Data, its usage, and its protection. This position carries significant legal and ethical obligations to ensure that data is handled in compliance with applicable laws and in a manner that respects the rights and privacy of Data Subjects.

13.4 Data Processor

The term "Data Processor" encompasses any organizational body or natural person, legal entity, public authority, or agency that is entrusted with the responsibility of processing Personal Data on the controller's behalf. Data Processors fulfill a critical function by executing the data processing tasks in accordance with the directives of the Data Controller. It is imperative that they conform to rigorous contractual and legal responsibilities, guaranteeing the secure, lawful, and regulatory-compliant processing of the data in accordance with the directives of the Data Controller.

13.5 Processing

The term "Processing of Personal Data" refers to a variety of manual and automated operations performed on collections of Personal Data or Personal Data. The operations encompassing data collection, recording, organization, structuring, and storage are indicative of the preliminary stages involved in data management. Further, it incorporates activities such as data modification or adaptation, information retrieval, consultation facilitation, data transmission or dissemination, and data disclosure. Additionally, it encompasses the provision of data to pertinent stakeholders, the organization or merger of disparate datasets, the imposition of limitations on data utilization, and, if required, the deletion or destruction of data. This all-encompassing definition underscores the wide range of activities entailed in the processing of Personal Data, all of which are required to be executed in adherence to pertinent data protection regulations in order to protect the privacy and rights of individuals.

13.6 Anonymization

"Irreversible de-identification of Personal Data" refers to a procedure in which the data is rendered anonymous, rendering it impossible to identify the individual, either by the Data Controller or another entity, using reasonable time, cost, or technology. After undergoing the anonymization procedure, the data no longer meets the criteria for Personal Data processing principles, as it is no longer designated as such. Due to the fact that anonymized data lacks any association with a specific identifiable individual, it is exempt from the regulations and restrictions that pertain to the management of personal data. By undergoing this transformation, privacy is effectively protected, and data protection principles are no longer applicable to the information in question.

14 Policy Compliance

14.1 Compliance Measurement

To ensure compliance with this policy, the Information Security Management Team will utilize a variety of verification techniques—including, but not limited to, the examination of business tool report analyses, the execution of internal and external investigations, and the proactive solicitation of feedback from the policy owner—among others. A robust system of checks and balances is maintained by these mechanisms in order to ensure that the policy's directives are consistently adhered to. Through the implementation of these all-encompassing strategies, the institution can uphold the utmost levels of information security, guarantee the efficacy of the policy, and proactively confront any possible domains for enhancement or non-adherence.

14.2 Exceptions

Any departure from this policy requires the Information Security Manager's prior approval and documentation. By following this procedure, it is guaranteed that exceptions are granted with discretion and in adherence to established protocols. In addition, the Management Review Team is dutifully informed of any authorized deviations, which promotes transparency and establishes a system for higher-level oversight and decision-making in order to uphold the policy's credibility and ensure its congruence with the goals of the organization.

14.3 Non-Compliance

Employees who are discovered to have violated this policy may be subject to disciplinary action, which may consist of warnings, suspension, or termination of employment, which is the most severe penalty. In order to underscore the gravity of policy infractions, uphold the integrity of the information environment, and guarantee adherence to legal and regulatory obligations, these measures are implemented. Infractions

are comprehensively examined and resolved in a manner commensurate with the gravity and context of the breach.

14.4 Continual Improvement

Consistent evaluations and revisions are implemented for this policy as a fundamental element of our perpetual process of enhancing operations. Regular evaluations and modifications guarantee that the policy maintains congruence with progressive technological developments, industry norms, and the constantly shifting information security environment. This strengthens our dedication to implementing strong data protection measures.

14.5 Compliance with ISO 27001

Our Data Protection Policy is in complete alignment with the globally acknowledged ISO 27001 standards, ensuring the implementation of strong information security controls and procedures. ISO 27001 functions as the fundamental pillar of our data protection strategy, establishing a standard by which we rigorously assess our endeavors. The subject matter comprises essential components, such as an effective incident response framework, access control measures to prevent unauthorized data access, and risk management to proactively identify and mitigate security risks. By adhering to this alignment, our dedication to protecting information, maintaining privacy, and mitigating cybersecurity risks is solidified, transcending mere rhetorical policy.

15 Awareness and Training

- Constant awareness and training regarding data protection will be made available to all personnel.
- Employees will be duly informed of their respective duties and obligations with regard to safeguarding data.
- Throughout the organization, data protection policies and procedures will be disseminated and comprehended.

16 Monitoring and Auditing

- Constant auditing and monitoring will be performed on data protection and management procedures.
- Audit records and files will be maintained for a specified time period and routinely reviewed.
- Periodically, compliance with ISO 27001 and data protection regulations will be evaluated.

17. Policy Review and Revision

Our dedication to safeguarding data extends beyond the mere execution of the policy. In order to align with the ever-changing data security environment and evolving industry benchmarks, this policy is subject to periodic evaluations and revisions, at a minimum once a year. Furthermore, we ensure compliance by promptly revising the policy in accordance with any modifications to data protection laws and regulations and maintaining a state of constant vigilance and responsiveness. Consistent evaluations and revisions guarantee the ongoing efficacy of our data protection protocols, thereby establishing and maintaining our organization's steadfast dedication to data protection. By maintaining a proactive and flexible approach, we strengthen our commitment to maintaining the utmost levels of data security and privacy, while also minimizing the potential hazards that arise from the constantly changing information security environment.

18 Conclusion

The Data Protection Policy serves as evidence of our steadfast dedication to protecting the core principles of data security, namely availability, confidentiality, and integrity. Within the ever-evolving digital environment, where data is critical to our functioning, this policy represents our commitment to safeguarding our priceless data assets against the constant dangers of illicit entry, disclosure, modification, or deletion. Through unwavering commitment to established norms and optimal strategies, most notably ISO 27001, our objective is to establish the preeminent benchmark for privacy and data protection in our field.

This policy is founded on the conviction that data protection is a continuous process rather than a fixed notion. Our dedication also encompasses the ability to adjust to the perpetually changing landscape of data security and privacy regulations. It is recognized that the digital realm is perpetually evolving, and we remain prepared to adapt our methodologies in response to emerging challenges.

Your inquiries and concerns are valued above all else. Please feel at liberty to contact us if you need any additional clarification, information, or documentation pertaining to our data protection policy and procedures. We are completely equipped to furnish you with the necessary insights and assurances. As a group, we shall persevere in our endeavor to uphold standards of excellence in data privacy and security, assuring all parties involved of our steadfast commitment to safeguarding their information.