DATA PROTECTION & SECURITY POLICY

Published

Version 7.1

Document Control	
Document Title	SP-POL-22-V7-Data Protection and Security Policy
Prepared By	Usman Haider, GRC Analyst
Reviewed By	Morola Akande, DPO
Approved By	M. Tariq Bashir Awan, CSO

Dissemination Control		
PU	Public	✔
INT	Internal — Company Use Only	
CON	Confidential — Limited to Relevant Groups	
RR	Restricted/Regulated — Access to Authorised Personnel	

Version Control			
Version No.	**Date Issued**	**Author**	**Update Information**
V1.0	June 06, 2019	CTO	First Published Version
V2.0	July 15, 2020	CTO	Revised Version
V3.0	March 02, 2021	Security Team	Revised Version
V5.0	December 12, 2022	Security Team	Revised Version
V6.0	December 05, 2023	Security Team	Revised Version
V7.0	May 13, 2024	Usman Haider	Revised Version
V7.1	Jan 16, 2025	Ezaan Abrar	Minor Update

Management Commitment

At Shufti Pro Limited ("SP," "we," "our," "us," or "the Company"), data privacy and integrity are core values embedded in our culture. As a leading identity verification (IDV) platform, we proactively embrace changes in data protection regulations, continuously evaluating and updating our security and privacy practices to exceed legal requirements. This commitment ensures that:

1. Our customers' data is fully protected, and
2. We support our customers in maintaining compliance with applicable Data Protection Laws.

SP operates as a Software as a Service (SaaS) provider, delivering end-to-end IDV services globally to various industries, including financial institutions, digital businesses, e-commerce, travel and hospitality, and blockchain enterprises. In line with the General Data Protection Regulation ("GDPR"), SP is dedicated to upholding the highest data protection standards.

Policy Updates and Privacy Practices

We have revised our Privacy Policy to align with GDPR requirements, ensuring it is clear and user-friendly for our customers and employees. Key initiatives include:

- **Annual Data Protection Impact Assessments (DPIAs):**
  - Mapping and analysing systems holding Personal Data to ensure GDPR compliance.
  - Adjusting processes across services, IT, sales, marketing, and HR to be GDPR-ready.
  - Evaluating sub-processors and services to maintain high data protection standards.
  - Reviewing and updating Data Processing Agreements as required.
- **Data Protection by Design and Default:**
  - Embedding privacy into our product and development lifecycle.
  - Utilising strong encryption and access controls to secure end-user data.

Data Transfers and Safeguards

For international data transfers, SP employs appropriate safeguards, such as the European Union's Standard Contractual Clauses ("SCCs"), to ensure data security. We have implemented robust technical and organisational measures, enabling our clients and users to confidently access personal information, even outside the EU.

Security and Compliance Standards

SP's infrastructure, data centres, and offices are evaluated against stringent security standards, including PCI-DSS, Cyber Essentials UK, and ISO 27001. These measures reinforce our commitment to the highest levels of data security.

Training and Awareness

To cultivate a privacy-conscious culture, SP conducts GDPR awareness training for information owners and sub-processors. This training equips individuals with the knowledge and skills required to manage Personal Data responsibly and comply with relevant Data Protection Laws.

Dedicated Data Protection Oversight

SP has appointed a dedicated Data Protection Officer (DPO) responsible for monitoring data protection practices, conducting periodic audits, and ensuring continuous compliance with GDPR and other applicable laws. Additionally, key personnel receive targeted training to remain updated on evolving regulatory requirements.

Commitment to Transparency and Excellence

This policy aims to provide a clear understanding of SP's data protection obligations and the measures we have in place to fulfil them. By prioritising transparency and accountability, we reinforce our commitment to safeguarding Personal Data and maintaining customer trust.

Morola Akande.

Data Protection Officer.

Shufti Pro Limited

1. Introduction

Shufti Pro Limited is strongly committed to protecting personal data. This Data Protection and Security Policy outlines the rules and principles by which the Company ensures ongoing compliance with data protection laws.

As set out in the GDPR, personal data refers to any information relating to an identified or identifiable living person. Shufti Pro processes personal data for various purposes, with the methods of collection, the lawful basis for processing, usage, disclosure, and retention periods differing for each purpose.

2. Interpretation and Definitions

2.1. Key Terms and Definitions

- **Automated Decision-Making (ADM)**: Decisions made solely on automated processing without human involvement, producing legal effects or significantly affecting an individual.
- **Automated Processing**: Use of personal data to evaluate or predict aspects of an individual (e.g., behaviour, location).
- **Company**: Shufti Pro Limited (SP), a company duly incorporated in the United Kingdom and governed by the laws of England and Wales.
- **Company Personnel**: Includes employees, consultants, directors, and other staff.
- **Consent**: Freely given, specific, informed agreement by the Data Subject for data processing.
- **Data Protection Laws:** Applicable laws, including GDPR and the UK Data Protection Act 2018.
- **Data Controller:** Entity determining the purposes and means of processing personal data.

- **Data Processor:** Entity processing personal data on behalf of the Data Controller.
- **Data Subject**: Identifiable living individuals whose personal data is processed.
- **Data Privacy Impact Assessment (DPIA)**: tools and assessments used to identify and reduce risks of a data processing activity. DPIA can be carried out as part of Privacy by Design and should be conducted for all major system or business change programs involving the Processing of Personal Data.
- **EEA**: the twenty-eight (28) countries in the EU, and Iceland, Liechtenstein and Norway.
- **Explicit Consent**: consent expressly confirmed in words;
- **General Data Protection Regulation (GDPR)**: the General Data Protection Regulation ((EU) 2016/679). Personal Data is subject to the legal safeguards specified in the GDPR.
- **Information Owner**: any employee personnel with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal.
- **Personal Data**: any information identifying a Data Subject or information relating to a Data Subject that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. Personal Data includes Special Categories of Data and Pseudonymised Personal Data but excludes anonymous data or data that has had the identity of an individual permanently removed. Examples of Personal Data include a name, email address, location, or date of birth.
- **Personal Data Breach**: Security breach leading to destruction, loss, or unauthorised disclosure of personal data.
- **Processing, Processed or Process**: any activity that involves the use of Personal Data. It includes collecting, recording or storing Personal Data, or carrying out any operation or set of operations on the data including organising,

amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring Personal Data to third parties.

- **Profiling:** automated processing of personal data to evaluate certain things about an individual.
- **Special Categories of Data**: Sensitive data such as racial origin, health, or sexual orientation.

3. Data Protection Objectives

The Objective of this policy is to ensure data protection in accordance with principles set out in the GDPR, which are the following:

- **Fairness and Lawfulness:** Data must be collected and processed legally and fairly.
- **Purpose Limitation:** Processing must align with the purposes defined before collection.
- **Transparency:** Data subjects must be informed about processing purposes, recipients, and other relevant details.
- **Data Minimization:** Process only necessary data; anonymise where possible.
- **Accuracy:** Ensure personal data is accurate and up-to-date.
- **Storage Limitation:** Retain data only as long as necessary, with justifications for extended retention.
- **Confidentiality and Security:** Protect data with appropriate technical and organisational measures.

4. Scope

- **Roles and Responsibilities**

  The responsibilities of the management, Data Protection Officer and Information Owners.

- **Documentation:**

Shufti Pro's requirements in respect of documenting processing under GDPR.

- **Data Protection by Design and Default:**

  Shufti Pro's requirements for Data Protection Impact Assessments.

- **Lawful Basis for Processing:**

  Shufti Pro's policy on maintaining accurate records of instructions provided by data controllers.

- **Security:**

  Policy measures designed to protect information confidentiality, integrity and availability of data/system/servers of Shufti Pro.

- **Contracts:**

  The measures that should be in place to ensure contractual relationships of Shufti Pro incorporate and maintain GDPR compliance.

- **International Transfer:**

  Oversight measures for international transfer of data by Shufti Pro.

- **Data Breaches:**

  Principles for detecting and responding to data breaches at Shufti Pro.

- **Training and Awareness:**

  Objectives for the training and awareness programme of Shufti Pro regarding data protection obligations.

- **Data Subject Rights:**

  Shufti Pro's obligations and response regarding individual rights of Data Subjects as enshrined in the GDPR.

- **Data Back-up and Storage:**

  Policy measures to outline the data back-up and recovery controls to ensure the integrity of data in the event of a hardware/software failure or physical disaster.

- **Changes to this Policy:**

  Policy updates and review procedure.

5. Roles and Responsibilities

- **Management:** Ensure adequate resources and governance for data protection.
- **Data Protection Officer (DPO):** Monitor compliance, conduct DPIAs, and serve as the point of contact for supervisory authorities.
- **Information Owners:** Establish and enforce data control measures.
- **Employees:** Follow data protection policies and report potential breaches.

6. Documentation

Shufti Pro maintains a Record of Processing Activities (ROPA) in line with Article 30 of GDPR. This includes:

- Controller and processor details.
- Processing purposes and categories.
- Retention periods.
- Technical and organisational security measures.

Documentation is reviewed regularly to ensure accuracy and compliance.

6.1. Policy Requirements

Where Shufti Pro acts as a Data Controller for personal data, it maintains documentation in a manner consistent with Article 30(1) of the GDPR:

- Name and contact details of the controller and, where applicable, the joint controller, the controller's representative, and the data protection officer;
- The purposes of the processing;
- A description of the categories of data subjects and the categories of personal data;
- The categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;

- Where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;
- Where possible, the envisaged time limits for erasure of the different categories of data;
- Where possible, a general description of the technical and organisational security measures referred to in Article 32(1).

Where Shufti Pro is a Data Processor for personal data, it maintains documentation in a manner consistent with Article 30(2) of the GDPR:

- The name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and, where applicable, of the controller's or the processor's representative, and the data protection officer;
- The categories of processing carried out on behalf of each Data Controller;
- Where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;
- Where possible, a general description of the technical and organisational security measures referred to in Article 32(1).

Shufti Pro must also document the following if it processes special category or criminal conviction and offence data:

- The condition for processing under the Data Protection laws; the lawful basis for processing; and
- Whether the Personal Data is erased and retained in accordance with Shufti Pro policy.

Shufti Pro shall conduct regular reviews of the personal data processed and update documentation accordingly.

7. Data Protection by Design and Default

Shufti Pro integrates privacy principles into processing activities by:

- Minimising processed data.
- Ensuring pseudonymisation and encryption.
- Conducting DPIAs for high-risk processing activities.

7.1. Policy requirements

Being a Data Processor, Shufti Pro shall implement technical and organisational measures that would facilitate its controllers in ensuring that Personal Data is processed to the highest standards of privacy protection (for example, only the data necessary should be processed, short storage period, limited accessibility, etc.) The ability to be pseudonymised (replacing personally identifiable material with artificial identifiers) and encrypted (encoding messages so only those authorised can read them). Personal Data shall be at the disposal of Shufti Pro's Controllers.

Shufti Pro shall carry out a Data Protection Impact Assessment ('DPIA') when:

- Using new technologies; and
- Where the processing is likely to result in a high risk to the rights and freedoms of individuals.

Processing that is likely to result in a high risk in the following situations (but is not limited to):

- Systematic and extensive processing activities, including profiling and where decisions that have legal effects or significant effects on individuals;
- Large scale processing of special categories of data or personal data related to criminal convictions or offences. This includes processing a considerable amount of personal data at regional, national or supranational level; that affects a large number of individuals; and involves a high risk to rights and freedoms e.g. based on the sensitivity of the processing activity.

8. Automated Processing (including profiling) and Automated

Decision-Making

Under the GDPR, Article 22, the data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, unless

a. A Data Subject has Explicitly Consented;

b. The Processing is authorised by law; or

c. The Processing is necessary for the performance of or entering into a contract.

8.1. Policy Requirements

The above-mentioned points (b) or (c) shall not be applicable if certain types of Special Categories of Data are being processed, however, this kind of data can be processed if processing is necessary for reasons of substantial public interest.

A demonstration of Explicit Consent is required for Processing Special Categories of Data, for Automated Decision-Making and for cross-border data transfers, unless there are other legal bases for processing.

9. Lawful Basis for Processing

Under the GDPR, there are six available lawful bases for processing as set out in Article 6 of the GDPR.

- **Consent:** the individual has given clear consent for processing their personal data for a specific purpose.
- **Contract:** the processing is necessary for a contract a Data Controller may have with the individual.
- **Legal obligation:** the processing is necessary for you to comply with the law (not including contractual obligations).
- **Vital interests:** the processing is necessary to protect someone's life.
- **Public task:** the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

- **Legitimate interests:** the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

9.1. Policy Requirements

Where Shufti Pro acts as a Data Controller, it shall ensure that data processing is performed on a legal basis as set out in Article 6 of GDPR. It shall further ensure that consent of the data subject is obtained fairly and straightforwardly, and that the data subject is made aware of its rights to withdraw its consent.

Where Shufti Pro acts as a data Processor, the lawful basis for processing must be ensured and communicated to Shufti Pro by the relevant Data Controller, according to whose instructions Shufti Pro shall process the Personal Data.

Regardless of its role as either a Data Processor or a Data Controller, Shufti Pro shall maintain a comprehensive Privacy Policy that informs prospective data subjects and customers regarding the collection, use or the storage of Personal Data.

10. Consent

GDPR sets out "consent" as any freely given, specific, informed and unambiguous indication of the Data Subject's wishes which is done through a clear affirmative action signifying agreement to the Processing of their Personal Data.

10.1. Policy Requirements

The affirmative action to Processing can either be done by a statement or positive action. Therefore, pre-ticked boxes, silence, or inactivity are not considered consent. Moreover, if the processing has multiple purposes, consent should be given for all of them separately.

According to GDPR, Article 7(3), Data Subjects shall have the right to withdraw Consent to Processing at any time. The withdrawal of the Consent shall not affect the lawfulness of the Processing based on Consent before its withdrawal.

11. Security Measures

Shufti Pro's Information Security Policy includes:

- Role-based access control and least privilege principles.
- Regular vulnerability assessments and updates.
- Secure backup and recovery processes.
- Incident management procedures for breach detection and mitigation.

11.1. Policy Requirements

Shufti Pro shall define and implement an **Information Security Policy** that underlines the security measures needed for supporting management systems to maintain effective and proportionate security. The IT policy shall regulate:

- **Responsibilities:** The individuals responsible for ensuring the security and integrity of information, servers as well as physical security of premises and workstations;
- **Software Policy**: Software licensing, installation and usage policies;
- **Physical access controls:** Controls established to prevent unauthorised physical access such as secure buildings and access controls within the premises to prevent unauthorised persons from gaining access to Personal Data and ensure third parties (such as operating data centres) are also adhering to such controls. Security incidents: Operating procedures designed to investigate is to identify, detect, investigate and resolve any suspected or actual data security breach.
- **Emergency management of Information technology:** Emergency response of Shufti Pro in case of website disruption, hardware failure, data deletion or other security breaches.

In addition to the above stated, Shufti Pro shall also ensure that the most advanced commercially sound security measures are in place to ensure data integrity and diminish security vulnerabilities. To this end Shufti Pro shall:

- ensure adequate physical and logical access control, using the following

principles: need to know, least privilege, role-based access control, segregation of duties, and complex authentication methods;

- control all changes in organisation, business processes, information processing facilities and systems that affect information security (and changes should be planned, tested prior to implementation and have rollback options);
- implement a vulnerability management process to determine the need for updates and patches to information processing systems;
- prevent and detect information leakage and compromise through a non-exclusive combination of firewalls, HIDS, NIDS, SIEM (which systems shall be kept up-to-date);
- separate the Personal Data and any type of backup of the Personal Data from any other data held by Processor in such a way as to prevent access to the Personal Data by other customers, clients, third parties or staff not involved in working with the Personal Data;
- implement a due diligence process on third parties that are contracted by Processor commensurate with the potential impact they might have on the security of the Personal Data.

12. Contracts regarding Third-Party Relationships

The GDPR requires diligence and clarity in entering into third-party relationships. Whether Shufti Pro is a Data Processor or Data Controller, there are mandatory requirements relating to the contracts that should be in place.

12.1. Policy Requirements

Whenever Shufti Pro acts as a processor a written contract must be in place with the controllers. Standards to be applied to the contracts have been elaborated upon by the Information Commissioner's Office, therefore, Shufti Pro shall:

- Only act on the Data Controller's documented instructions, unless required by law to act without such instructions;
- Ensure that people processing the data are subject to a duty of confidence; take

appropriate measures to ensure the security of processing;

- Only engage a sub-processor with the controller's prior authorisation and under a written contract;
- Take appropriate measures to help the controller respond to requests from individuals to exercise their rights and in meeting its GDPR obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments;
- On an annual basis review third-party relationships to determine the risk posed to processing. This will be documented as a part of a DPIA. Based on this assessment, the DPO will determine the most appropriate means to validate that contractual obligations in relation to data processing are being adhered to.

13. International Transfers

Restricted transfers outside the UK or EEA are permitted only with:

- Adequacy decisions.
- Standard contractual clauses or other safeguards.
- Explicit consent from data subjects where necessary.

All international transfers are recorded and reviewed by the DPO.

13.1. Policy Requirements

Shufti Pro may, subject to the Data Controller's consent, transfer personal data for purposes integral to its business subject to adequate safeguards. Individuals' rights must be enforceable and effective legal remedies for individuals must be available following the transfer. Shufti Pro shall incorporate the following adequate safeguards for transfer of data outside EEA:

- Standard data protection clauses in the form of template transfer clauses adopted by the European Commission;

- Explicit consent of the data subject based on Shufti Pro Privacy Policy made available to each data subject before collection of Personal Data.

The DPO shall record instances of international transfer of Personal Data in the Data processing register. The DPO prior to allowing any transfer of data internationally, will consider the resultant impact on data subject rights and the appropriate means of adopting safeguards.

14. Data Breaches

Shufti Pro's breach response protocol includes:

- Immediate reporting to the DPO.
- Assessment of the breach's impact.
- Notification to the ICO within 72 hours if required.
- Direct communication with affected individuals for high-risk breaches.

14.1. Policy Requirements

The DPO must be notified of all breaches to this Policy as soon as possible pursuant to which the DPO shall record breaches and work with the Information owner to consider the likely impact of the breach. Where a breach is considered notifiable to the Information Commissioner, the DPO shall immediately inform the same within seventy-two (72) hours of Shufti Pro becoming aware of it.

- The notification shall contain the nature of the personal data breach including;
- The categories and approximate number of individuals concerned; and
- The categories and approximate number of personal data records concerned;
- The name and contact details of the DPO or other contact point for more information; a description of the likely consequences of the personal data breach;
- A description of the measures taken, or proposed to be taken, to deal with the personal data breach; and
- Where appropriate, of the measures taken to mitigate any possible adverse effects.

Where a breach is likely to result in a high risk to the rights and freedoms of individuals, Shufti Pro will notify those concerned directly. All employees must be trained to recognise and escalate breaches.

A detailed **Data Breach Policy** governs any instances of data breach and provides adequate guidelines for Shufti Pro employees in such an instance.

15. Training and Awareness

Employees undergo annual and induction training on:

- GDPR principles and compliance requirements.
- Cybersecurity best practices.
- Data breach recognition and escalation.

Training metrics are monitored and reported to ensure effectiveness.

15.1. Policy Requirements

Employees must be trained on the requirements of this Policy at least annually through the annual compliance training and the induction training for new joiners. The employees shall be trained to ensure that:

- They can identify the range of potential problems, both general and specific;
- Have a clear understanding of the consequences of their actions;
- Are able to establish procedures that can be (and are) consistently adhered to;
- Are aware of the compliance requirements, not just the GDPR, but also general cyber security, payment security standards (PCI DSS) and ISO.

16. Individual Rights

Shufti Pro upholds GDPR rights, including:

- **Right to Access:** Provide access to personal data within one month.
- **Right to Rectification:** Correct inaccuracies promptly.
- **Right to Erasure:** Delete data upon request where applicable.

- **Right to Restrict Processing:** Limit processing under specific conditions.
- **Right to Data Portability:** Provide data in a machine-readable format.
- **Right to Object:** Cease processing for direct marketing or other purposes unless overriding legitimate interests exist.

Requests are managed by the DPO and logged for transparency.

16.1. Policy Requirements

Although Shufti Pro, acting as a sub-processor, is only liable to abide by the instruction of the relevant data controller, it shall endeavour to allocate data subjects their rights under the data protection legislation; subject to the controls provided by the relevant Data Controller.

Making a request for personal data shall be free unless a reasonable cost is to be charged where requests are unfounded, excessive or repetitive in character.

Regarding the data subject's right to be informed, Shufti Pro maintains a **Privacy Policy** and publishes this publicly. This outlines how Shufti Pro collects, processes and disseminates the data. All data subjects are made aware of this policy before their data is collected.

All requests from subjects for access to their data should be submitted immediately to the DPO using the *Request Form - Data Subject Access* attached at the end of the Privacy Policy (https://shuftipro.com/privacy-policy/). The DPO shall log the request and will:

- Consider whether the request is manifestly unfounded or excessive;
- Request copies of information held from Information owners within Shufti Pro
- Review the information to ensure it does not impair the privacy of another data subject;
- Consider whether the request warrants a fee (if it requires a significant amount of data); and
- Respond to the original request.

A response to the request shall be provided without delay and at the latest within one (1) month of receipt. In the event the request is particularly complex or numerous, the period of compliance can be extended by a further two (2) months. If this is the case, the DPO must inform the individual within one (1) month of the receipt of the request and explain why the extension is necessary. Performance against the response target of one (1) month must be reported to the Board by the DPO at least annually.

Requests for rectification must be treated in the same way as requests for access. The following, additional, measures will apply:

- If Shufti Pro has disclosed the Personal Data in question to third parties, the DPO shall inform them of the rectification where possible. The DPO must also inform the data subject about the third parties to whom their data has been disclosed where appropriate.
- The information owner will be responsible for ensuring the request for rectification of the information they are responsible for is actually made.
- The DPO shall be responsible for validating whether requests for rectification have been properly addressed.

Requests for the erasure of data by any data controller or data subject should be submitted immediately to the DPO and will follow the same principles as for right to access and right to rectification.

If Shufti Pro has disclosed the personal data in question to third parties, the DPO must inform them about the erasure of the personal data, unless it is impossible or involves disproportionate effort to do so.

Requests for data under the right to data portability must be submitted to the DPO. The DPO is responsible for recording these and requesting the information from the information owner(s).

The DPO will also review the data to ensure the privacy of other data subjects is not adversely impacted. The DPO will provide the personal data in a structured, commonly used and machine-readable form, submitted using a secure transfer mechanism. The information will be provided within one month of the original

request.

17. Data Back-up and Recovery

All computer systems maintained by the Shufti Pro must be backed up on a regular schedule. These systems are typically servers but are not necessarily limited to servers. Servers expected to be backed up include the file server, the mail server, and the web server. The backup media will be stored in a secure off-site location. The off-site location can include “cloud” computer storage. It shall be ensured that data backups are conducted continuously, and the backed-up data is kept secure on a separate backup server so that it can be utilised in case of any emergency.

The purpose of the systems backup is to provide a means to:

- Restore the integrity of the computer systems in the event of a hardware/software failure or physical disaster, and;
- Provide a measure of protection against human error or the inadvertent deletion of important files.

Shufti Pro uses SSAE-compliant and ISO 27001-certified data centres across the globe for our secure data backups with AES-256-CBC or an encryption technique of equivalent strength.

Shufti Pro shall implement a quarterly program of back-up testing to ensure that backed-up data will be available when required. After each series of testing a review shall be undertaken and any areas for improvement identified shall be implemented as appropriate.

Shufti Pro has a **Data Breach Policy** which must be followed after every security related incident. This Policy gives a framework for the investigation and reporting of the issue as well as the identification of mitigating actions to prevent the recurrence of a similar issue in the future, see Shufti Pro Data Breach Policy for details.

18. Changes to this Policy

To obtain the latest version of this policy, please refer to the portal regularly. We reserve the right to make amendments to this Policy at any time without notice.

18.1. Approval and Review Procedure

This policy is reviewed annually by the DPO and CSO. Amendments are communicated to employees via the company portal.