ShuftiPro

Data Protection and Security Policy

Version 2.0

Data Protection and Security Policy for Shufti Pro Limited

Document Control	
Prepared By	Leah Oskar
Approved By	Shahid Hanif
Reference Documents	Shufti Pro Data Protection and Security Policy

Version Control			
Version Number	**Date Issued**	**Author**	**Update Information**
V1.0	August 7, 2018	Leah Oskar	First Published Version
V2.0	July 15, 2019	Leah Oskar	Revised Version

Dissemination Level		
PU	Public	☒
PP	Restricted to other program participants.	
RE	Restricted to a group specified by the company participants.	
CON	Confidential, only for members of the company.	

Management Commitment

Data privacy and integrity have always been the core value of Shufti Pro Limited's (the "**SP**") culture. As a leading identity verification platform we fully embrace the upcoming changes; evaluated and update our data security as well as privacy practices to exceed the requirements set forth by the Data Protection Laws. We do this to ensure that (i) our customers' data is fully protected; and (ii) we are supporting our customers to be compliant as well.

SP is a Software as a Service (SaaS) solution provider which provides end-to-end identity verification ("**IDV**") services to businesses globally. As an IDV service provider to numerous customers including financial institution(s), digital businesses, e-commerce, travel & hospitality, and block chain, SP is committed to the principals of General Data Protection Regulation (the "**GDPR**").

We have revised our Privacy Policy in line with the GDPR to make it clearer and easier for our customers as well as our employees to read and comply with.

We, further, undertake annual data protection impact assessments (**DPIA**) in order to:

- Map and analyse all systems holding Personal Data in order to make all systems GDPR-compliant;
- Adjust processes handling Personal Data (such as services, information technology, sales, marketing, human resources) to make processes GDPR Ready;
- Evaluate services and our sub-processors where we process Personal Data for our customers; and
- Review and update Data Processing Agreements where needed.

Understanding that all our end-users are data subjects and that protecting their Personal Data is paramount,SP has embedded the principle of data protection by design and default, as mandated by the GDPR and elaborated by the Information Commissioner's Office, UK (the "**ICO**"), into its product and development lifecycle. Strong encryption and defined access control are key techniques which assure that our customers' data, specifically end-user's data, is secure.

As to the transfer of data, if any, we use appropriate safeguards such as the European Union's ("**EU**") Standard Contractual Clauses (the "**SCC**"). We have implemented appropriate technical and organisational measures to ensure stringent data security so that our users or clients can feel confident that personal information is safe and secure when accessed even from outside the EU.

Parallel to the GDPR implementation, SP has evaluated all its data centres, offices, and infrastructure based on PCI-DSS, Cyber Essentials UK, and ISO 27001 requirements to ensure the best possible security of Personal Data. GDPR awareness trainings have also been carried out for Information owners across SP and its sub-processors.

To ensure continuous data protection and fulfilment of GDPR's requirements, SP has a dedicated Data Protection Officer in charge of monitoring data protection practices and periodic audits. Moreover, it is ensured that individuals in charge of specific functions at SP have the requisite training and awareness regarding the Data Protection Laws.

This policy is drafted so that the reader may, first, be made aware of the obligations posed by the relevant Data Protection Laws and then is made aware of the policies in place at SP.

___(signed)___
Mr. Shahid Hanif,
Data Protection Officer.
Shufti Pro Limited.

1. Data Protection Objectives

- Fairness and lawfulness:
  When processing Personal Data, the individual rights of the data subjects must be protected. Personal data must be collected and processed in a legal and fair manner.

- Restriction to a specific purpose:
  Personal Data can be processed only for the purpose that was defined before the data was collected. Subsequent changes to the purpose are only possible to a limited extent and require substantiation.

- Transparency:
  The data subject must be informed of how his/her data is being handled. In general, personal data must be collected directly from the individual concerned. When the data is collected, the data subject must either be aware of, or informed of:
  a. The identity of the Data Processor;
  b. The purpose of data processing;
  c. Third parties or categories of third parties to whom the data might be transmitted.

- Data reduction and data economy:
  Before processing personal data, it must be determined whether, and to what extent, the processing of Personal Data is necessary in order to achieve the purpose for which it is undertaken. Where the purpose allows and where the expense involved is in proportion with the goal being pursued, anonymized or statistical data must be used. Personal data may not be collected in advance and stored for potential future purposes unless required or permitted by relevant data Controller.

- Deletion:
  Personal Data that is no longer needed after the expiration of legal or business process-related periods must be deleted. There may be legal obligation that merit protection or instructions by data Controller in individual cases. If so, the data must remain on record until the interests that merit retention have expired.

- Factual accuracy:
  Up-to-datedness of data Personal Data on record must be correct, complete, and – if necessary – kept up to date. Suitable steps must be taken to ensure that inaccurate or incomplete data are deleted, corrected, supplemented or updated.

- Confidentiality and data security:
  Personal Data is subject to data secrecy. It must be treated as confidential on a personal level and secured with suitable organizational and technical measures to prevent unauthorized access, illegal processing or distribution, as well as accidental loss, modification or destruction.

2. The Scope of this Policy

- 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 integrity of data in the event of a hardware/software failure or physical disaster.

3. Roles and responsibilities

Shufti Pro has appointed Muhammad Shahid Hanif as the 'Data Protection Officer' ('**DPO**") pursuant to, and in compliance of, Article 37 of the GDPR.

The DPO's responsibilities in line with Article 39 of GDPR:

- Informing and advising Shufti, its affiliates and sub-processors about their obligations to comply with the GDPR and other data protection laws.
- Monitoring compliance with the GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments; train staff and conduct internal audits.
- Acting as the first point of contact for supervisory authorities and for individuals whose data is processed (employees, clients etc.) and for any individual who wishes to report any breach of data protection obligations.
- Monitoring performance and providing advice on the impact of data protection efforts.
- Maintaining comprehensive records of all data processing activities conducted by the company, including the purpose of all processing activities, which must be made public on request.
- Interfacing with data subjects to inform them about how their data is being used, their rights to have their personal data erased, and what measures the company has put in place to protect their personal information.

4. Documentation

As per Article 30 of the GDPR, Controllers, as well as Processors, or their representatives are bound to maintain a record of processing activities under their responsibility.

Policy requirements:

Where Shufti Pro acts as a 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 of 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 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 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 updates documentation accordingly.

5. Data protection by design and default

The need for privacy by design. Privacy (and Data Protection) by design and by default is written into Article 25 of the EU GDPR. In essence, appropriate technical and organisational measures are to be implemented that integrate data protection principles and safeguard individual rights into the processing activities.

<u>Policy requirements:</u>

Being a data processor Shufti Pro shall implement technical and organisational measures which 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 of pseudonymise (replacing personally identifiable material with artificial

identifiers) and encrypt (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 relation 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.

6. Lawful basis for processing

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

a. Consent: the individual has given clear consent for processing their personal data for a specific purpose.
b. Contract: the processing is necessary for a contract a controller may have with the individual.
c. Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).
d. Vital interests: the processing is necessary to protect someone's life.
e. 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.
f. 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.

Policy requirements:

Where Shufti Pro acts as a data Controller it shall ensure that data processing is performed on legal basis as set out in Article 6 of GDPR. It shall further ensure that consent of data subject is obtained in a fair and straightforward manner, and that 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 who's 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 which informs prospective data subjects and customers regarding the collection, use or the storage of Personal Data.

Furthermore, Shufti Pro shall undertake to seek consent from each data subject regarding processing of their Personal Data. Such consent shall be

7. Security

The GDPR requires personal data to be processed in a manner that ensures its security. This includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage. It requires that appropriate technical or organisational measures are used.

Policy requirements:

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

- Responsibilities: The individuals responsible for ensuring 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 unauthorized 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 investigation 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 any 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 organization, 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.

8. Contracts

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

Policy requirements:

Whenever Shufti Pro acts as a processor a written contract must be in place with the processors. 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;
- delete or return all personal data to the controller (at the controller's choice) at the end of the contract, and the processor must also delete existing personal data unless the law requires its storage; and
- submit to audits and inspections including providing the controller whatever information it needs to ensure they are both meeting their Article 28 obligations;
- On an annual basis review third party relationships to determine the risk posed by 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.

9. International transfers

The GDPR imposes restrictions on the transfer of personal data outside the European Union, to third countries or international organisations. These restrictions are in place to ensure that the level of protection of individuals afforded by the GDPR is not undermined. The GDPR, however, allows international transfer of Personal Data subject to 'adequate safeguards'.

Adequate safeguards may be provided for by:

- a legally binding agreement between public authorities or bodies;
- binding corporate rules (agreements governing transfers made between organisations within in a corporate group);
- standard data protection clauses in the form of template transfer clauses adopted by the Commission;
- standard data protection clauses in the form of template transfer clauses adopted by a supervisory authority and approved by the Commission;
- compliance with an approved code of conduct approved by a supervisory authority;
- certification under an approved certification mechanism as provided for in the GDPR;
- contractual clauses agreed authorised by the competent supervisory authority; or
- provisions inserted into administrative arrangements between public authorities or bodies authorised by the competent supervisory authority.

Policy requirements:

Shufti Pro may, subject to 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.

10. Data breaches

A Personal Data breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

The GDPR introduces a duty on all organisations to report certain types of data breach to the relevant supervisory authority. In some cases, organisations will also have to report certain types of data breach to the individuals affected.

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 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.

11. Training and awareness

A key condition of the GDPR is that employees, who are in receipt of Personal Data, are fully informed of the rights and responsibilities of data subjects. Moreover, all personnel shall be properly trained so as to minimize the chances of data breaches from within the organization. that accidental data loss, which comprises unintended losses like improper disposal and database misconfiguration, do not compromise data security and integrity.

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.

12. Individual rights

One of the key changes brought about by the GDPR which businesses must be aware of is how individuals' rights in respect of their personal data have been affected. The GDPR aims to give individuals (whether these be customers, contractors or members of staff) more control over the ways in which businesses process their personal data.

For the purposes of data processing done by Shufti Pro, the following rights under GDPR are to be protected and engrained:

- The right to be informed
- The right of access
- The right to rectification
- The right to erase
- The right to data portability

Individuals have the right to access their personal data and supplementary information. The right of access allows individuals to be aware of and verify the lawfulness of the processing.

Under the GDPR, individuals will have the right to obtain:

- confirmation that their data is being processed;
- access to their personal data; and
- other supplementary information – this largely corresponds to the information that should be provided in a privacy notice.

The GDPR also gives individuals the right to have personal data rectified if it is inaccurate or incomplete.

The right to erasure is also known as 'the right to be forgotten' is meant to enable an individual to request the deletion or removal of personal data where there is no compelling reason for its continued processing. However, the right to erasure does not provide an absolute 'right to be forgotten'. Individuals have a right to have personal data erased and to prevent processing in specific circumstances. These include:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed.
- When the individual withdraws consent.
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing.
- The personal data was unlawfully processed (i.e. otherwise in breach of the GDPR).
- The personal data has to be erased in order to comply with a legal obligation.
- The personal data is processed in relation to the offer of information society services to a child.

The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.

The right to data portability applies:

- to personal data an individual has provided to a controller;
- where the processing is based on the individual's consent or for the performance of a contract; and
- when processing is carried out by automated means.

Policy requirements:

Although Shufti Pro, acting as a sub-processor, in 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 relevant data controller.

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

Regarding data subject's right to be informed, Shufti Pro maintains a **Privacy Policy** and publishes this publically. 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 month of receipt. In the event the request is particularly complex or numerous, the period of compliance can be extended by a further two months. If this is the case, the DPO must inform the individual within one month of the receipt of the request and explain why the extension is necessary. Performance against the response target of one 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 is 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 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.

13. 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 utilized 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 certified data centres across the globe for our secure data backups with either AES 128-bit, AES 256-bit or 448-bit Blowfish encryption.

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.

Definitions

- "Data Protection Laws" means all applicable laws relating to the processing of Personal Data including, while it is in force and applicable to Client Data, the General Data Protection Regulation (Regulation (EU) 2016/679), as well as, the Data Protection Act 2018;
- "Personal Data" has the meaning given to it under the General Data Protection Regulation (Regulation (EU) 2016/679);
- “Information Owner” means 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.
- Data Subject means is any natural person whose data can be processed. In some countries, legal entities can be data subjects as well.
- ‘Controller’ means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data;
- ‘Processor’ means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;
- ‘Consent’ of the data subject means any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;
- ‘DPIA’ means a privacy-related impact assessment whose objective is to identify and analyse how data privacy might be affected by certain actions or activities.
- ‘Personal Data Breach’ means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.