Shufti Pro

# CROSSING PATHS:
# KYC VERIFICATION & GDPR

## Under the Dome

The Effectiveness of Data Processors

in Correlation to GDPR

# Introduction

Some years ago, a documentary titled **Under the Dome** was released to the public that showcased the rapid decline in air quality and pollution across the world, east asia in particular. The central theme around the documentary inspired realisation and awareness amongst people about the inherent destructive outcomes on the environment.

GDPR possesses the same importance in magnitude and scale in terms of data and privacy laws across the European Union. It ensures to protect and empower the EU citizens' data privacy and the outlook of organisations across the region, towards personal data.

However, most companies are unaware of the apparent financial and reputational repercussions that the failure of GDPR implementation might cause for them.

Entities and Organizations that rely on third party service providers represent a significant liability on account of digital identity verification. According to the GDPR, data subjects can introduce claims against controllers directly. Whether as data processor or data controller (in cases of non-compliance), either of them can be made to provide compensation to the data subjects.

When looked at from a financial, regulatory and reputational standpoint, companies stand at a delicate position of exposing their compliance shortfalls.

This handbook is written to provide informative awareness and guidance to prospective customers about the processor and their compliance fulfillment measures.

Concerning the regulatory environment around the world and the tightening financial security solution. Companies need to be in position of command with appropriate questioning towards processors and their claims of being GDPR compliant.

**This e-book will facilitate companies to enquire their data processors about GDPR compliance.**

# Background Into GDPR

## What is GDPR?

General Data Protection Regulation is a directive set by the European Union. A legislation that sets forth guidelines regarding the 'personal information' collected and how it is processed and used of EU citizens. In the pretext of GDPR, EU citizens are referred to as 'Data Subjects'.

## Who is it meant for?

The GDPR legislation was formed to harmonize data privacy laws across Europe. Empowering all EU citizens' data privacy in the process, GDPR is aimed at reshaping organisations' approach towards data privacy.

Basically the GDPR applies to all businesses and entities that are operating in the EU and all regions under its jurisdiction. In addition, the GDPR also applies to entities operating outside of EU jurisdictions. How, you'd ask? Companies operating outside of the EU but still dealing in the personal information of data subjects (EU Citizens) will be subject to all guidelines of the GDPR effectively; this includes data processors and controllers as well.

## Personal Information or Personal Data

The definition of 'personal data' is entirely different to what people think, with respect to the word 'Personal Information' or PII, which is fairly commonly used in North America. PII includes narrowed down information, such as full name, address, date of birth, social security number and financial information such as credit card numbers or bank accounts. According to the GDPR, 'Personal Data' covers a much wider range of information that can include social media posts, photgraphs, preferences and even credit/ debit transaction histories. It is very crucial to know the difference between the two, where Personal Data can include PII, but PII in most cases cannot include Personal Data.

# Debate of Data Processor & Data Controller

When speaking in reference to the GDPR, data processor and data controller hold their own unique representation and responsibility, accordingly to which, each entity is held accountable.

## Who is a Data Processor?

The primary responsibility of the data processor is to process personal data on behalf of a controller. Data processors are usually third party entities that process information.

## Who is a Data Controller?

A data controller determines the purpose for which and the means by which that personal data is processed.

## Who are we then?

Shufti Pro as a service provider will be considered a third party service entity, who will be considered a data processor. We are the company, who will be processing personal data of data subjects on behalf of the controller, who decides to implement Shufti Pro.

## What makes you then?

You are a company that implements the directives and guidelines set by the GDPR. As a result you create measures, policies and improvements that conform to the GDPR and determine how and which data will be processed. This makes you the rightful acting Data Controller.

Data processors also carry some crucial responsibilities. In particular, GDPR expresses that the data processor:

- Acts in accordance to the data controller's documented instructions.
- Makes sure that concerned people handling personal data need to be informed about confidentiality.
- Ensures adequate and proper security measures for data protection.
- Needs to go in accordance with regulations for sharing information in third countries.
- Needs to assist data controllers, where possible, in providing facilitation for data subject rights measures.
- Assists the data controllers in obtaining approval from the relevant DPOs.
- Returns or deletes all record of personal data post data processing activities, on the controllers request.
- Can be held accountable in non compliance to contractual obligations.

To best achieve GDPR compliance and to establish a strong partnership, processors and controllers must have a co-developed strategy for processing and handling the data of their customers and users.

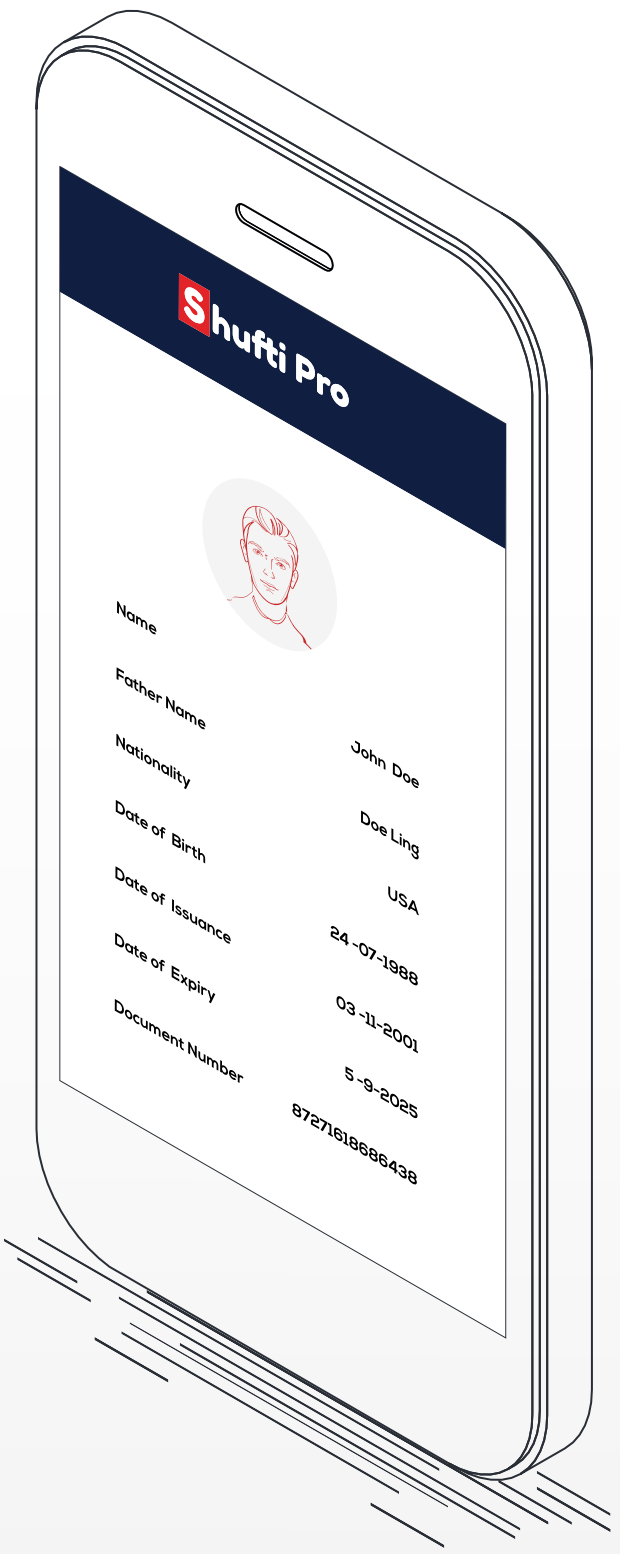
# GDPR and Shufti Pro for IDV

When speaking in reference to the GDPR, data processor and data controller hold their own unique representation and responsibility, accordingly to which, each entity is held accountable.

## Identity Verification - The Present

Given that most businesses that run today are conducted online, the process of validating the identity of a person holds even more importance. In the absence of in-person verification, the element of trust is drastically minimised. As there is a definite lack of connection between a person's digital and physical identity. Providers such as Shufti Pro are employed to bridge this very gap.

It is crucial to know that GDPR holds strict scrutinization for entities that process personal data. This includes PII data and other information that can violate the rights of a data subject including identification information (Electronic Copies of Image, ID cards, Payment Card Information, etc.).


## KYC to be Unaffected by GDPR

GDPR doesn't restrict the KYC operations of a company, rather recognizes the importance of identity and ensures its protection. GDPR, at it's core, merely emphasises better protection of data subjects (EU Citizens), by directing how information is collected, processed and used.

Companies in contact with such information, will need to ensure the security of information in a manner that conforms to the GDPR guidelines. Additionally, they need to make the use of information very clear, easy to understand and transparent for individuals.

# Shufti Pro - Complying to the GDPR | Step By Step

Shufti Pro respected (and continues to respect) users' privacy and data security long before the GDPR came into effect. While this might be the outward expression echoed by many data processors, Shufti Pro has been long under practical work. To establish transparent and simple practices that define processes and procedures through effective documentation.

In order for Controllers to implement trustworthy Processors, the right way forward is to choose the ones who are ready with GDPR adherences, practically and to the fullest!

# How Shufti Pro Complies to GDPR

Shufti Pro acknowledges government regulations, directives and believes in showcasing transparent responses, in accordance to the GDPR directives for clearer and improved customer viewability and understanding.

## Data Transfer

The GDPR provides data access rights to data subjects. This ensures data security and improved data protection measures while empowering the data subject to enact upon their rights.

Having the flexibility to customise data transfer is important in exercising GDPR requirements. A solution that can adapt along the way, ensuring that during a data cycle, the relationship between the data subject and service provider is not effected at the trust level.

### Retention

Adhering to the GDPR, Shufti Pro holds only relevant PII data, images and electronic copies of individuals having undergone verification through our platform. All personal data is held on dedicated, self-hosted servers, located in classified locations within the EEA Zone.

### Erasure

All personal data is the property of the legal user. A user may request personal data to be deleted upon request. Accepting responsibility and accountability, we facilitate such queries promptly.

### Request Back

At any given time, a user may request their data from the processor. Shufti Pro will facilitate in providing back the data in question, in appropriate and standard formats to the user, in a clustered collection.

# Data Security

Service providers or data processors need to ensure data security through adequate measures to minimize the likelihood of data breaches, whether pre-emptive or post. Data breaches and protection of data itself come under the wider umbrella of the data lifecycle.

Additionally, GDPR calls for secure auditory practices to be carried out, to ensure standardized operations and encryption practices during data breaches. New techniques are preferred for GDPR compliance.

## Data Breaches

According to article 33.2, GDPR calls for the processor to notify any data breach to the controller upon knowledge. On part of Shufti Pro, we intimate any breach in data servers promptly, to the concerned individual representing the controllers side. This is done through any mutually agreed digital communication medium as immediately as possible.

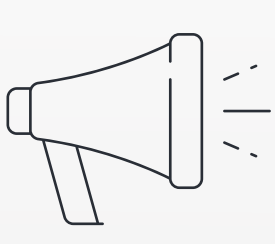
## Data Protection

All personal data is securely transmitted in a TLS encryption only through dedicated API calls during transit. There is no data stopover in between calls and responses from the server during the transmission. Shufti Pro stores all the data in an SHA256 encrypted format, where data is held on multiple server locations to ensure backup existence and data loss recovery. All servers are backup-ready every fourteen minutes to maximise security and save up-to-date data.

# Data Subject Rights - Consent Management

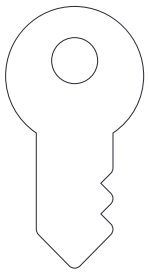
Service providers or data processors need to ensure that data subjects are fully provisioned to exercise their rights and are well aware of them. All documentation and support materials need to be properly maintained in a transparent manner for data subjects.

The GDPR provisions for data subjects, mentioned through articles 12-23 of the 'Rights of the Data Subject', states exclusive privileges granted to data subjects across a range of accountabilities.



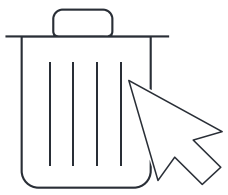
## Right to be Informed

Data subjects are provisioned as per GDPR to be duly notified by the processor with appropriate documentation regarding information pertaining to all processes and activities. Shufti Pro ensures to provide transparency to the Controller and end-user, by providing easy-to-understand documentation and procedure notifications beforehand.



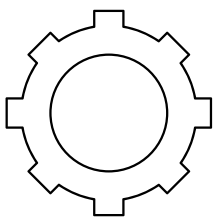
## Right to Access

End-user has the right to access data, when they seek in requirement of so. Shufti Pro shall provide the user with data and information, where it deems is a legitimate requirement of what the user has requested for.



## Right to Erasure

According to the GDPR, users can request to have their data erased. Shufti Pro respects the rights of data subjects and the directives that GDPR enforces. Upon request, the concerned data of the subject individual is erased from our systems and all backup holdings entirely.

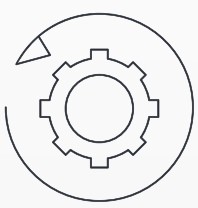


## Right to Restrict Data Processing

Users have the authority to convey to the processor and enquire about the nature of processing on their data and accordingly restrict further processing to take place. If they deem that a certain process is unnecessary or unlawful, the data is inaccurate or the purpose of data retention is reasonless on behalf of the controller, users have the right to restrict data processing.

## Right to Object

The data subject possesses the rights to object, on grounds relating to their situation in particular. This may include profiling or contacting for purposes of marketing. Shufti Pro does not use any collected information for the purpose of marketing as it would violate the purpose and intent for rightful information collection, which is for KYC purposes, as defined.



## Right Not to Automatic Profiling

A data subject has the right to not be subjected to a decision based solely on automated processing, including profiling. Shufti Pro, as a processor, possesses no legal authority or command to label or profile a data subject based on automated processing.

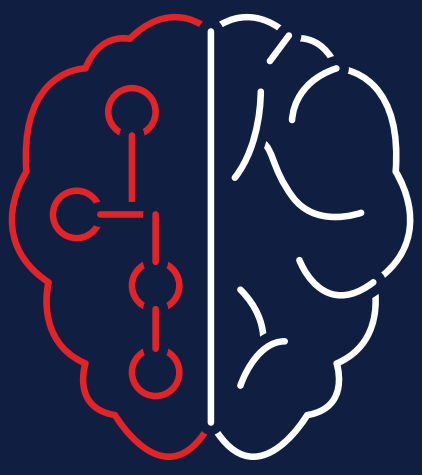
# Incorporating The Element of Human Intelligence

As more IDV solutions become automated and key components of the verification cycle are performed by the AI and programming logic, there is an increased doubt on the effectiveness of such automated solutions that constitute to trust deficits. Consumers are left with a lack of understanding of the viability of such a solution.

Though IDV solutions are automated and the results can be constituted as an 'automated decision'. The approval of such processes and activities, should be sought prior to taking consent from the end-user, as stated in article 22, clause 2 part **"based on the data subject's explicit consent."**

Having a human element to an IDV solution is more permissible and acceptable for data subject adherence and cooperation towards the verification process. Since the GDPR gives data subjects the rights to not be subject to decisions solely on automated decisions. Human intervention is somewhat of a mandatory pursuance for service providers to comply to.

Since a data subject can request their data or object to the processing entirely, enquire the purpose and intent for processing, human involvement facilitates data processors in providing a more informative response. This ensures explanations are more timely and thorough in justification, for ambiguous verifications, data inconsistencies and 80 percent or less AI confidence scores.



## Shufti Pro - Striking the Right Balance between HI & AI

Shufti Pro has clearly separated the elements of HI and AI to ensure non-intrusive operations. Both elements work in conjunction for the fulfilment of the identity verification process. The processing of logic, comparisons and cycle is left for the AI to perform, whereas HI is involved minimally for human review purposes and problem rectification. Holding no doubts on our AI capacity, Shufti Pro incorporates HI experts as a second layer of security, from the commencement of a verification process as effective vigilance. Shufti Pro's hybrid approach ensures that AI and HI duo centrally amplify the transparency and effectiveness of the solution.

# Making An Impact

Shufti Pro is one of the youngest verification service providers that has emerged as an industry player in a relatively short span of time. During this period, not only has Shufti Pro acquired GDPR compliance, but PCI DSS as well. Shufti Pro reflects the effectiveness of its services, through its policies, internal mechanisms and procedures. The way industry recognition reflects the completion of its adherence to GDPR specific guidelines and measures, is a testament to controllers and end-users of our service capability.

| Category | Our Measures |
|---|---|
| Security | ● End-to-end data encryption during journey; military grade encryption at server storage (idle)<br>● Annual and randomised security audits, penetration tests, back-end vulnerability testing<br>● PAN masking at all times<br>● Immediate notification to controller on data breaches |
| Data | ● Minimised time period for data storage according to industry requirement only |
| Self Preparation | ● Adequate and up-to-date process documentation and literature for review<br>● Consent measures and content provided in a transparent manner |

## Proof Of Verification: Secure Evidentiary Practice

As an IDV provider, staying ahead of the curve by keeping client data safe is a fundamental requirement in today's competitive industry. This is of interest to controllers, in order to assess data processors based on their effectiveness and reliability. The global regulatory environment emphasises evidentiary proof, especially in a high-risk segment of Identity Verification & Management. Proof of Verification happens to be a service offering rare to come by for data processors to provide.

We, at Shufti Pro, offer proof of verification as a way to securely record the entire KYC process of a particular user as a continuous video stream. Additionally, random screenshots are captured at key times during the KYC process from the beginning till the end.

Proof of verification facilitates legal investigation and criminal proceeding by providing real evidentiary proof to authorities in cases where evidence of value are required.

# Conclusion

## A Relationship of Great Importance:

For companies, if you deal in the recording of personal information, which includes PII data or identity information from data subjects, they are subject to guidelines and directives set by the GDPR. The GDPR clearly outlines the strict enforcement on data controllers and the subsequent responsibilities that they can be held accountable for. However, the GDPR also outlines specific areas of responsibility that befall the processors, if found in breach of the GDPR.

GDPR is no longer under the dome; it is for us all to realise that GDPR is here to stay. Both, controller and processor play a crucial role in the effective functioning of a solution and the eventual reaching of goals in data protection and privacy. As our systems become smarter, the greater goal is to integrate real identities with digital identifies and bridge the gap between them, through a dedicated online verification service provider as a processor.

Holding such an important position, it should be understood that IDV companies be properly and thoroughly assessed. Ensure that the service complies to the GDPR fully and no such deficiency at the processors' end create legal hindrances for you.

We anticipate this e-book has brought insight to you about the GDPR in general, Shufti Pro's stance, and the know-how required to assess your IDV vendors with better knowledge pertaining to data security and protection.

Stay on the top with a data processing solution that is as versatile, dependable and reliable, as you seek!