

2021/06/25

Dear Client

## POPI Act compliance

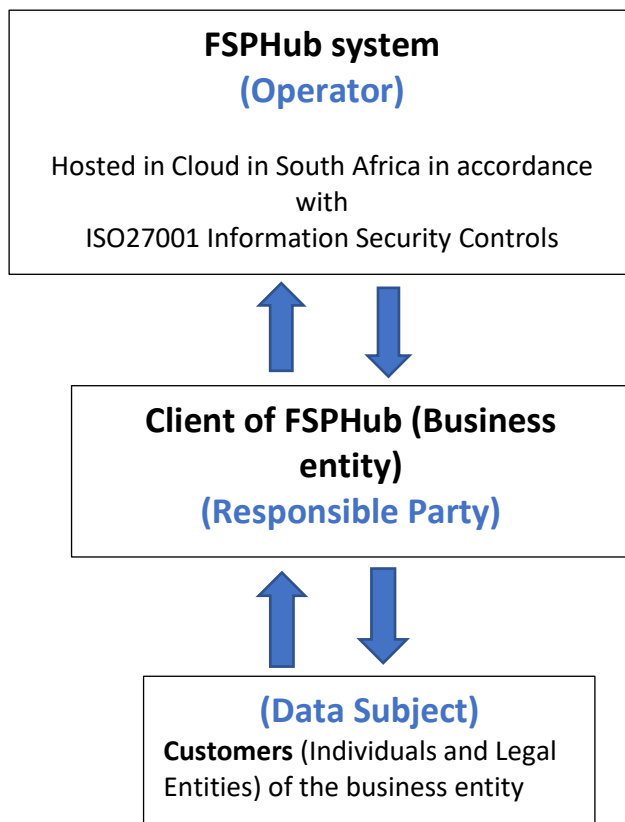
In terms of the Protection of Personal Information Act, 2013 (Act 4 of 2013) (POPIA), and Promotion of Access to Information Act which comes into effect on 1 July 2021, all private and public bodies processing personal information, are required to have implemented policies and procedures in order to be compliant.

Hubit (Pty) Ltd t/a FSPHub has appointed an Information Officer as prescribed by POPIA, who has overseen the implementation of the Protection of Personal Information Act, 2013 (Act 4 of 2013) (POPIA).

The function of the Information Officer is to ensure that the information provided by the data subject is only used for the intended purposes, it is supplied for. The Information Officer is to ensure that all policies and procedures are always followed and adhered to.

How will POPIA and PAIA be implemented and what is the flow of information within the FSPHub software solution?

We have simplified the role players in accordance with POPIA in the diagram below:



### The Operator (FSPHub)

1. FSPHub provides businesses (Responsible Party) with access to a web-based Practice Management System. System access is username and password protected.
2. The Operator (FSPHub) **does not** process nor transfer any data to third parties on behalf of Responsible Party.
3. The FSPHub system is hosted in a Secure Cloud environment located in South Africa.
4. In accordance with Data Security Protocols, the FSPHub system undergoes security vulnerability and penetration testing to identify potential risks and implement risk mitigation procedures.
5. Data breach protocols are established in accordance with the requirements of POPIA.
6. The FSPHub system facilitates notification to Responsible Parties and Data Subjects in event of a breach. It is the RESPONSIBILITY of the Responsible Parties to notify THEIR and Data Subjects of ALL Security Breaches
7. FSPHub is not obligated by Law to provide Copies of POPIA Policies, Controls, Procedures, Processes and Artifacts that were created to meet their UNIQUE requirements, which are in accordance with THEIR Executive Directives, and hence will not be in Accordance with the UNIQUE requirements of any other third party.

### The Responsible Party

System access is provided to the business (Responsible Party) so that business processes, documents, and communication with their customers (Data Subject) are managed in accordance with the Stipulations of both POPIA and PAIA Acts.

It is incumbent on the Responsible Party to be compliant with both POPIA and PAIA Act's in accordance with the Scope as determined by the Regulator.

The Responsible Party is SOLELY Accountable for the Collection, Processing and Management of their Clients (Data Subjects) Personal Identifiable Information (PII)

### The Data Subject

The Data Subject is in essence the Client of the Responsible Party.

It is incumbent of the Responsible Party to ONLY Collect Personal information in respect to the nature of the Services being provided.

This, in accordance with the Act includes.

1. Full Names and Surname
2. Identity Number
3. Email
4. Phone Number
5. Physical address – if required for the explicit purpose of providing a Service on premises
6. Banking details – if required for creation of Debit orders etc. Where Data Subject pays CASH, this IS NOT a requirement

In the event of ANY additional Information requirements the Responsible Party is to apply to the Regulator in Accordance with the Section 57 (1) and 58 (2) of the Act in respect of Unique Identifiers

Yours sincerely,



**Sean Barrett**  
CEO & Information Officer