StructureIt

IT PRIVACY POLICY

Version 1.1

December 2017

DOC#: SIT-GRP-GRP-021

CONTENTS

Compiled by	Quality Review	Approved By
Murray Woolfson	Ryan Kuhn	Llewellyn Watson
Date:27/03/2017	31/03/2017	15 May 2017

1. Document Approval

The following roles within StructureIt Ltd are required to approve any updates to this policy, before any communication or enforcement of policy statements can be effected.

Authorised By	Name	Signature	Date of Approval
Director (SA office)	Llewellyn Watson		19 December 2017

2. Document Review Register

Date	Reasons for Review	Change Description	Name of reviewer
31-Mar-17	Quality Control	Review	Ryan Kuhn
04-April-17	Quality Control	Format Document	Ryan Kuhn
11-Apr-17	Quality Control	Review	Sarel Blignaut
5-May-17	Quality Control	Amendments required	Ryan Kuhn
9-May-17	Quality Control	Comments added	Llewellyn Watson
15-May-17	Quality Control	Additional Content added	Ryan Kuhn
15-May-17	Quality Control	Finalisation	Llewellyn Watson
12-December-17	Amendments	Add European Union to disclaimer	Ryan Kuhn
19 December 17	Quality Control	Finalisation	Llewellyn Watson

3. Distribution Schedule

Role	Business Function
Director (UK)	Director
Director (MAU)	Director
Director (NZ)	Director
Director (ZAR)	Director

4. Introduction

The following framework aims to identify and guide the StructureIt group of companies with respect to the data processing considerations unique to their business service delivery. The framework considers acquisition of data from clients, processing, transformation, migration and final return and disposal of the data within the software development environment.

5. Privacy Policy

Privacy policy refers to platforms and solutions designed, developed and wholly owned by StructureIt whereby user personal information is obtained, stored and processed, existing and in development. The privacy policy also refers to the collection of personal information of all its employees, staff, service providers and contractors across the StructureIt group of companies. Where insofar possible, local privacy laws must be adhered to with regards to solutions deployed that collect personal information.

Consent to collect personal information
StructureIt owned solutions which collect personal information must make provision for the communication of "consent to collect personal information" which is readily available and accessible to users of the solution. Consent must confirm the collection, use and disclosure of personal information failing which if consent is not given the user must not use the solution.

Personal information of staff, employees, contractors and service providers collected in respect to the recruitment or procurement process of StructureIt will only be for the purposes of recruitment or supplier vetting as per the on-boarding procedure and procurement process of StructureIt.

Limitations on Collection, Use and Disclosure
StructureIt owned solutions which collect personal information must make provision for the communication of the limitations thereof insofar as to the notice of data processing of personal information if so requested, the collection of information for specific, limited purposes and the relevance thereof, the processing of personal information with the purpose for which is was intended for. The necessary steps to ensure the information is reliable, accurate, complete and kept-up-date.

Disclosure of personal information to third parties
StructureIt owned solutions which collect personal information must make provision for the communication of any required or intended disclosure of personal information insofar as to the transfer or disclosure thereof to identified third parties and the option made available to opt-out of said disclosure.

Security of Personal information
StructureIt owned solutions which collect personal information must make provision for the communication of the security of personal information and the reasonable attempts in which each respective system aims to provide the security thereof to avoid the unauthorised disclosure, misuse, alteration or access thereof.

Access to Personal information
StructureIt owned solutions which collect personal information must make provision for the communication of the access to personal information by advising the user what procedure to follow in order to access their information per system.

Retention of Personal Information
StructureIt owned solutions which collect personal information must make provision for the communication of the retention requirements for each respective platform as is necessary in order to provide the service.
All personal information obtained and stored within any StructureIt owned system is also subject to the Data Processing Framework that is enforced across the StructureIt network.

6. Applicability

This document is applicable to all users, contractors or suppliers within the StructureIt business who make use of or have access to personal information both in development environments and production environments. The privacy policy applies to all personal information contained within the StructureIt environment including wholly owned proprietary StructureIt systems and databases. Where privacy legislation requirements exist within a region, it is important to confirm adherence thereto and for the StructureIt IT representative to confirm compliance.

7. Website Privacy Disclaimer and Content

The StructureIt Group of Companies are extremely committed to protect your privacy and confidentiality. We understand that our clients, are quite rightly concerned to know that their data will not be used for any purpose unintended by them, and will not accidentally fall into the hands of a third party. We endeavour to guard against any unauthorised access to your data, however, when it comes to data transmission over the internet, there can be no guaranteed that it will be completely secure. In order to safeguard your data, all inbound and outbound communication to and from the servers, utilise a digital certificate for encryption, over the secure sockets layer protocol, (SSL). Our policy is both specific and strict. It complies with the Privacy principles laid out by South Africa, United Kingdom, Mauritius, New Zealand and the European Union.

The following references to the principles apply:

http://www.theforumsa.co.za/forums/showthread.php/19844-Eight-Principles-of-POPI

https://ico.org.uk/for-organisations/guide-to-data-protection/data-protection-principles/

http://dataprotection.govmu.org/English/Documents/Presentation/OvervDPA.ppt

https://privacy.org.nz/news-and-publications/guidance-resources/information-privacy-principles/

https://www.mthreeconsulting.com/blog/2017/04/the-6-privacy-principles-of-gdpr

The StructureIt Group of Companies endeavours to uphold the following privacy and security principles in any and all engagements with our clients:

Accountability

The responsible person must ensure that the Privacy and Security Principles are followed and adhered to.

Fair and Lawful Purpose

You must:
Have legitimate grounds for collecting and using the personal data;
Not use the data in ways that have unjustified adverse effects on the individuals or company concerned;
Be transparent about how you intend to use the data.
Handle individuals or company's personal data only in ways they would reasonably expect;
Make sure you do not do anything unlawful with the data.

Adequacy and Relevance

Personal data shall be adequate, relevant and not excessive in relation to the purpose for which they are processed. So, you should identify the minimum amount of personal data you need to properly fulfil your purpose. You should hold that much information, but no more. This is part of the practice known as "data minimisation".

Processing Limitation

Must be lawfully processed, in a reasonable manner.
May only be processed if it is adequate, relevant and not excessive.
Must have been consented to and collected directly from the subject (subject to provisions)

Further Processing Limitation

Must be in accordance with the purpose for which it was collected
Responsible party must take account of the relationship between purpose of intended further processing and the initial purpose of collection.

Information Quality and Accuracy

Responsible party must take reasonable practicable steps to ensure information is complete, accurate and not misleading.
It must be updated where necessary and take into account the purpose for which collected.

Retention

Personal data processed for any purpose shall not be kept longer than is necessary for that purpose or those purposes.

Storage and Security

Responsible party must secure the integrity and confidentiality of personal information in its possession or under its control.
Take reasonable technical and organisational measures to prevent loss of, damage, unlawful access or unauthorised destruction.
This includes risk management and steps to identify threats.
The Regulator/Information Commissioner and Subject must be informed if there has been or a reasonable expectation of a breach of security.

Openness and Respect of Privacy Rights

Responsible party must take reasonable practical steps to ensure the Subject is aware of the information being collected, the purpose and the source.
A right of access to a copy of the information comprised in their personal data;
A right to request the correction or deletion of personal information that is inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully.
A right to object to processing that is likely to cause or is causing damage or distress;
A right to prevent processing for direct marketing;
A right to object to decisions being taken by automated means;

A right in certain circumstances to have inaccurate personal data rectified, blocked, erased or destroyed; and a right to claim compensation for damages caused by a breach of the Act.

Control Over Trans Border Data Flows

Personal data shall not be transferred to another country, unless that country ensures an adequate level of protection for the rights of data subjects in relation to the processing of personal data.

Unique Identifiers

Unique identifiers - such as IRD numbers, bank customer numbers, driver/s licence and passport numbers - must not be assigned to individuals unless this is necessary for the organisation concerned to carry out its functions efficiently. The identifiers must be truly unique to each individual (except in some tax related circumstances), and the identity of individuals must be clearly established. No one is required to disclose their unique identifier unless it is for, or related to, one of the purposes for which the identifier was assigned.

Changes to the Policy

If there are any amendments to this policy, we will post the amendments on our website so that you are aware of what they are.