Privacy Policy

Document Control

Document Title	Privacy Plan Policy Manual
Purpose	This document is the submission for the Privacy Plan Policy for the Varsun.
File Name	privacy_plan_policy.doc
Prepared by	Hari

Revision History

Document Version #	Author	Section, Page(s) and Text Revised
1.0	Hari Sayyaparaju	

Table of Contents

1 Overview

The privacy of your data is important to us. This document will describe our information practices and the measures we take to protect your data to comply with applicable laws and our obligations.

2 Purpose

Varsun eTechnologies collects and processes client information that may be subjected to privacy practices. This document will detail how we approach securing this data and our practices and policies to ensure privacy of any sensitive data is achieved.

3 Scope

This document will detail how we collect, receive, access, use and disclose data that we receive through enterprise hosting, SaaS, remote managed services and other analytics offerings. We will also detail how Varsun eTechnologies governs the use of this data to provide offerings to customers pursuant to our agreements with them.

4 Policy

4.1 Client-Customer Information includes details about the customer base related to the specific client. These details may include sensitive personal information, such as contact details, financial information, personal health, clinical trial data, demographic data, purchase history, and employee/employer related information. This data is collected by the client and stored within our enterprise software, however this data is never exported out of the client system instance and is never utilized by Varsun for whatever purpose.

We operate under the assumption that it is the client's obligation as a data controller to notify individuals whose personal data may be included in their database, detailing to them how they collect the data and the purpose for which they collect it. We have no direct relationship with the individuals whose personal data is included in customer Information we process.

We collect and process customer information only for the purpose of providing services to the client and in accordance with our agreements with client. In certain situations, we may supplement customer information provided by client with information from other sources. This is done only when specifically requested, and we agree to, such supplementation. This supplementation of customer information is for the sole purpose of providing services to the client. We will retain customer information for the duration stipulated in our agreement with the client, or longer, as necessary to comply with our legal obligations, resolve disputes or enforce our agreements.

4.2 Client Information is personal data about people in the specific client organization who we are providing a service to. This includes account managers and users, who interact with Varsun eTechnologies and its systems. Client information usually is limited to name, work email address, work phone number and job title. We collect information through online forms, email, phone and other written means that client use to provide it to us. We use client information to support client account, maintain our business relationship with client, respond to client inquiries and perform accounting functions.

Client information may also include User Information. User information is information generated by computers that interact with our systems. User information may be collected through the following:

4.2.1 Web server logs

In the process of administering this site, we maintain and track usage through web server logs. These logs provide information, such as what types of browsers are accessing our sites, what pages receive high traffic and the times of day our servers experience significant load. We use this information to improve the content and navigation features of our sites. Anonymized or aggregated forms of this data may be used to identify future features and functions to develop for the site and to provide better customer service.

4.2.2 Cookies and other tracking technologies

There are various tracking technologies, including "cookies", which can be used by us to provide tailored information from a website. A cookie is an element of data that a website can send to client browser, which may then store it on client system. Some Varsun eTechnologies systems may use cookies for authentication and security and/or to remember user settings so that we can better serve client when client return to those systems. By using those systems, client agree that we can place these types of cookies on client system. We can set their browser to notify them when you receive a cookie, giving client the chance to decide whether to accept it. Client can control the use of cookies at the individual browser level. For more information, they can refer to the user information provided with their web browser. If client reject cookies, they may still use Varsun eTechnologies systems, but their ability to use some features or areas of those systems may be limited.

We may also use User Information to help us prevent and detect security threats, fraud or other malicious activity, and to ensure the proper functioning of our products and services.

Varsun eTechnologies may additionally use Customer Information and Client Information for the following purposes:

- To maintain and upgrade a system Our technical staff may require periodic access to services data that may include Customer Information or Client Information, to monitor system performance, test systems, and develop and implement upgrades to systems. Any temporary copies of such services data created as a necessary part of this process are maintained only for time periods relevant to those purposes.
- To address performance and fix issues. On occasion, we may develop new versions, patches, updates and other fixes to our programs and services, such as security patches addressing newly discovered vulnerabilities. In accordance with the terms of client order for services, we may remotely access a user's computer, while that user observes, in order to troubleshoot a performance issue.
- To meet legal requirements Varsun eTechnologies may be required to provide personal data to comply with legally mandated reporting, disclosure or other legal process requirements when we believe, in our sole discretion, that disclosure is necessary to protect our rights, or to respond to a government request.

4.2.3 Third-Party Websites

If requested by client, and agreed to by Varsun eTechnologies, Varsun eTechnologies systems may be configured to enable client and its users to access other third-party websites whose privacy practices may differ from those of Varsun eTechnologies. If client or client's data subjects submit personal data to any of those websites, such information is governed by their privacy statements. We encourage client and their data subjects to carefully read the privacy statement of any website client or client data subjects access through our systems.

4.2.4 Data Access and Correction; Choices for Limiting Use and Disclosure

The US Privacy Shield Frameworks require that US data subjects have rights to access personal data about themselves that an organization holds and, more specifically, a right to:

1) obtain confirmation whether personal data about them is being processed;

2) have the data communicated to them so they may verify its accuracy and the lawfulness of the processing;

(3) have the data corrected, amended or deleted.

With respect to Customer Information, we operate under the assumption that it is client obligation as data controller to provide their data subjects a means of accessing their data and requesting that such data be corrected, amended or deleted. Under our current business model,

we have no direct interaction with client data subjects and so have no direct way for them to submit these requests to us. If you are a Varsun eTechnologies customer, and you receive such a request from a data subject about whom we host personal data, and you would like our assistance in responding to that request, please contact our privacy office at hr@varsun.com or Legal Division/Privacy Officer, Varsun eTechnologies, Aneheim, CA 92808, USA. We will respond to requests within 30 days of receipt.

With respect to Client Information, certain Varsun eTechnologies systems enable users to access and amend or correct their own personal data. Otherwise, if you or your users would like to request access to or correction of Client Information, please contact our privacy office at hr@varsun.com or Legal Division/Privacy Officer, Varsun eTechnologies, Aneheim, CA 92808, USA.We will respond to requests within 30 days of receipt.

We will not use or disclose Client Information for purposes that are materially different than those described in this Policy, or subsequently authorized, without offering data subjects a choice to opt out of such uses or disclosures.

4.3 Data Security

We take reasonable measures that are designed to protect personal data from loss, misuse and unauthorized access, disclosure, alteration and destruction. Some of our security measures include the following:

- **Security policies.** We design and support our products and services according to documented security policies. Each year, we assess our policy compliance and make necessary improvements to our policies and practices.

- **Employee training and responsibilities.** We take certain steps to reduce the risks of human error, theft, fraud and misuse of our facilities. We train our personnel on our privacy and security policies, and we require our employees to sign confidentiality agreements. We also have assigned to an individual the responsibility to manage our information security program.

- **Access control.** We limit access to Customer Information to only those individuals who have an authorized purpose for accessing that information. We terminate those access privileges following job change or termination.

- **Data encryption.** All electronic transfers of non-public Customer Information between client and Varsun eTechnologies(including sensitive personal information and sign-on credentials) are required by Varsun to be done through encrypted connections.

- **Azure AD.** As we use Azure AD and it enables SSO to SaaS applications, regardless of where they are hosted. Some applications are federated with Azure AD, and others use password SSO. Federated applications can also support user provisioning and password vaulting. Access to data in Azure Storage is controlled via authentication. Each storage account has a primary key (storage account key, or SAK) and a secondary secret key (the shared access signature, or SAS).

If we confirm that your Customer Information has been accessed or used by unauthorized individuals, we will contact your designated representative to coordinate our response to the incident. If you have any questions about the security of your personal information, you can contact us at hr@varsun.com or Legal Division/Privacy Officer, Varsun eTechnologies, Anaheim, CA 92808, USA.

4.4 Onward Transfers to Third Parties

We will not disclose personal data to third parties for purposes other than those described in this Policy, except at your direction and with your authorization. Disclosures of USA and India Personal Data will be carried out in accordance with Privacy Shield requirements relating to onward transfers. We will not sell, rent or lease your personal data to others.

5 Related Standards, Policies and Processes

None.

6 Definitions and Terms

None.

7 Revision History

Date of Change	Responsible	Summary of Change
March 2018	IT Privacy Team	