Privacy Policy

Last updated: 15 April 2022

This policy together with Our Usage Policy & Terms of Service forms part of and completes the Subscriber Agreement, which is applicable to all Services and products "Services" sold, offered or contracted to customers by DT Cloud Technologies "DTCT"

This Privacy Policy describes Our policies and procedures on the collection, use and disclosure of Your information when You use the Service.
We use Your Personal data to provide and improve the Service. By using the Service, You agree to the collection and use of information in accordance with this Privacy Policy.
Our data collection and usage procedures are aligned and compliant with the POPIA.

For any information, questions or data requests regarding this Privacy Policy, please contact Our appointed information officer:

Jeandre du Toit
0213001374
jdt@dtcloud.co.za

Interpretation

The words of which the initial letter is capitalized have meanings defined under the following conditions.
The following definitions shall have the same meaning regardless of whether they appear in singular or in plural.

Definitions

For the purposes of this Privacy Policy:

- **Account** means a unique Account created for You to access Our Service or parts of Our Service.
- **Company** (referred to as either "the Company", "We", "Us" or "Our" in this Agreement) refers to DT Cloud Technologies Pty Ltd "DTCT".
- **Cookies** are files stored on Your Device, which contains usage information related to Our Website.
- **Country** refers to: The Country You are currently connecting from.
- **South African Law** means all and any laws, policies, codes of conduct and or regulations of the Republic of South Africa.
- **Device** means any Device that can access the Service such as a computer, a cellphone or tablet.
- **Personal Data** is any information that relates to an identified or identifiable individual.
- **Service** refers to Our Website, features, Services and products.
- **Service Provider** means any natural or legal person who is authorized to process data on behalf of the Company.
- **Subscriber Agreement** refers to a legally binding contract, which is agreed to when signing up for any Service.
- **Usage Data** refers to non identifiable data that is collected automatically.
- **Website** refers to Our Website: **dtcloud.co.za**
- **You** (also referred to as “User”, “Subscriber” or “Customer”) means the individual Account holder accessing the Service.

Payment Information

In no circumstance do We store Your payment information such as Credit Card or CVV numbers.
All payment events and payment data is processed and stored solely by Our payment providers, who are accredited by PCI-DSS status.
Our payment providers may initiate automated fraud checks or require user verification based on the payment data You provide.

We make use of the following payment providers and methods, some or all of which may be or not be active and available for use at anytime:

- Payfast
- PayPal
- SnapScan
- Yoco
- Direct EFT

Personal Data

When signing up for Your first Service, We will ask You to provide some required personal information.

We use Your personal information solely for the purposes of providing the Service, agreements, authorization and in order to contact You.
The following personal information will be requested when signing up for a Service, however We may contact You if further information is required:

- Email address
- Phone number
- First and last name
- Residential Address, Area Code, City, Province/State, Country

Usage Data

Usage Data is collected automatically when using the Service.

Usage Data is non identifiable information, and is not linked to Your Personal Data in any manner.
We utilize Usage Data solely for the purposes of improving Our visitors browsing experience.

Types of Usage Data listed below:

- Public IPv4/6 addresses - To gather geolocation statistics of Our visitors.
- Page visits - To gather statistics of Website usage in general.
- Device information - To gather statistics of Our visitor's Device types.
- Software information - To gather statistics of browser types used to access Our Services.
- Usage patterns - To gather statistics on usage patterns such as time spent on a specific page.

Cookies

Utilizing Cookies is a method used to store data relating to Our Service, on Your local Device.

You must accept the use of persistent Cookies before any data will be stored.
We utilize Cookies for the following purposes only:

- Session Cookies - Saving data such as shopping cart, live chat and Website activity. Deleted when Your browser is closed.
- Persistent Cookies - Loading data such as Your Website preferences and saved login credentials. Deleted by You only.

Use Of Personal Data

We may use Your personal information solely for the following purposes:

- To initialize and provide the Service to You.
- To authenticate You as the registered Account holder, and user of the Service.
- To contact You via Email or Phone, in the event an action is required on Your Account.
- To provide You with news, promotions and other forms of non Account related communications, unless You have opted out of these communications.
- For support purposes, such as responding to issues related to Your Service.
- For billing purposes, such as sending invoices to Your Email address.

Sharing Of Personal Data

We may share Your personal information in the following situations:

- With Our authorized Service Providers in the event of them auditing, monitoring, analyzing or otherwise, the Service, and there is a requirement to contact You.
- With Your explicit written consent for any other reason.

Disclosure of Personal Data

The Company reserves the right to disclose Your Personal Data to 3rd party entities strictly under the following conditions.
Should any Personal Data be disclosed as described below, We will contact You to inform You of such event, and advise You to review the entities privacy policy.

- Where the Account holder may be or becomes classified under the Personal Data processing exclusion sections in the POPIA.
- To comply with a legal obligation such as a court order requesting Personal Data.
- To protect and defend the rights or property of the Company.
- To prevent or investigate possible breach of the Usage Policy or Terms Of Service in connection with the Service.
- To protect the personal safety of users of the Service or the public.
- To protect against any legal liability.

Retention of Personal Data

The Company will retain Your Personal Data only for as long as is necessary and in accordance with Section 14 of the POPIA.

In the event that You terminate all Services, resulting in Account closure after 30 days of no active Services, We will only process Your Personal Data as follows:

- Personal Data will be removed from Our active client's database, and will no longer be available for use by Our Service Providers.
- Personal Data will be archived only for as long as is required by any legal obligation, and in accordance with the POPIA regulations.

Securing of Personal and Sensitive Data

Data security policies and procedures are taken very seriously at Our organization. We require Our staff, Service Providers and other authorized entities to maintain compliance at all times.

All technical and data operations follow various authorization procedures, security technologies, code of conduct and non disclosure agreements amongst others:

- Our Website and portals are protected by SSL technologies, and all data communication sent and received within Our domain is encrypted by these technologies.
- We implement security technologies such as brute force detection, cross reference prevention, blacklisted geolocation zones and more across Our Services.
- All 3rd party modules, applications and features used by Our Services have been audited where possible, and inspected for any bugs or misconfigurations.
- Service related authentication data follows an isolation procedure, and is only accessible by the Customer.
- Authentication data will always and only be provided to Account holders in an encrypted manner.
- All Account related activities and support requests requires authorization from the registered Account holder.
- Any sensitive data due for removal from Our systems follow a 2 step data elimination method: Transfer to offline encrypted storage, deep format of offline storage.
- Our Usage Policy outlines prohibited usage, and We proactively take measures to ensure the Usage Policy is adhered to.
- We implement a zero trust policy in Our organization, as such any sensitive data or operations are only accessible by authorized individuals.
- We implement a code of conduct, non disclosure agreements, POPIA compliance training and industry related best practice procedures within Our organization.

Handling of Personal and Sensitive Data

It is important to note that We will never ask You either verbally, by written request or otherwise for or to perform any of the following data/actions:

- Your Account or Service authentication data, such as username's or password's.
- Your banking details, credit card numbers or otherwise, unless such request for data was initiated by You.
- Any additional Personal Data than what You have already provided to Us by signing up for a Service, or any data related to people You may know.
- To visit any link to change credentials, sign up for a Service, provide any type of data or otherwise, unless such request for action was initiated by You.
- To provide access to Your Service, Device or otherwise, unless such request for action was initiated by You.

Please ensure that Your visits, and all communications to and from Us are to and from the legitimate sources listed below:

- **Website** - https://dtcloud.co.za & https://portal.dtcloud.co.za
- **Calls & WhatsApp messages** - 0213001374
- **Emails** – support/accounts/ops/notifications @dtcloud.co.za

Please peruse Our security tips below to ensure minimal possibility of Your Account or Service being compromised:

- We kindly request that You change as soon as possible, any authentication data provided to You through Us.
- Keep software on all devices and Services up to date at all times.
- Make use of antivirus, antimalware and firewall software on all devices and Services.
- Use strong passwords of at least 8 characters, with a mixture of lower/uppercase, numbers and symbols.
- Do not use the same passwords on external 3rd party services.
- Do not use any Device that You suspect may be compromised, such as when ads and fake Service links are popping up on the display.
- Do not log into or make use of Your Account or Service while using public wifi, unless You are connecting through a VPN tunnel.
- If any communication You receive seems potentially harmful, unexpected or misplaced, please contact Us for verification before interacting with the communication.

Liability and Account holder responsibility

DTCT takes every reasonable and feasible effort with the technologies and methods available to ensure complete data security.

We assure Our clients that all platforms, services, modules, applications and others are under constant monitoring and receive updates as they become available.
In the event of a data compromise, We will notify all affected Account holders as soon as is reasonably possible detailing the event and possible remedies if required.

We can not accept any liability in the event of the following scenarios, where DTCT acted responsibly and these scenarios did not result from gross negligence on Our side.

- Data compromised due to software, where no exploit reports or fixes were provided by the vendors at least 90 days prior leading up to the compromise.
- Data compromised due to theft from Our or Our Service Providers' premises or platforms.
- Data compromised due to a system, Service, application or otherwise operation hosted by an Account holder

The Account holder is responsible and liable for any data compromised in the following scenarios:

- As a result of the Account holder sharing their or others' authentication data with another entity or with the public.
- As a result of the Account holder sharing their or others' Personal Data with another entity or with the public.
- In the event the Account holder's Device used to access the Service being or becoming compromised.
- Where the Account holder hosts, provides or otherwise makes available any software on the Service that is vulnerable or outdated.
- Due to a configuration made by the Account holder on their Service, which results in the Service becoming vulnerable.

External Services

Our Service may contain external links to other websites, services, documentation or otherwise information that is not in Our control.
When visiting such sites, Our Privacy Policy no longer applies. We strongly advise Our clients to view the privacy policy of all websites they visit.