

December 2016

Data Security in the GLOPortal Community Management System (CMS)

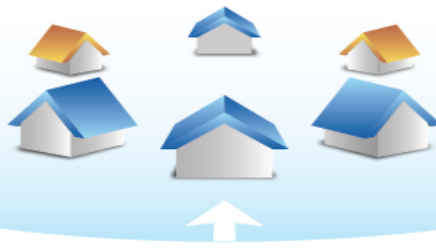
The protection of client's data is of critical importance to GLOvent Solutions. Handling sensitive client data is part of our core business and our right to exist would be threatened if we did not handle client data with the utmost care.

We have received and dealt with client data since the start of the company in January 2007. We have since handled information of multiple clients, with our current client base currently exceeding 650 communities, representing more than 130,000 database members. We are proud to say that to date we have not lost any of our client's data and are not aware of any technical leakages.

POPI (Protection of Personal Information) – we have received many enquiries as to our POPI compliance, firstly it must be noted that the POPI bill is not yet in effect, it will come into effect by proclamation by the President in the Government Gazette. It must be further noted that on the date when the President proclaims POPI into effect, all organisations will still have minimum 1 year to comply with the provisions of POPI. We are in the process of assessing the POPI bill and will be engaging with subject matter experts to ensure our POPI compliance when the bill comes into effect. **We are comfortable though that our GLOPortal CMS adheres to the core principles of data security which are generally accepted and also covered by the POPI bill.**

On a high level, the following **Technical measures** are in place to protect client data:

1. GLOvent currently monitors security recommendation's, standards and best practices from organisations such as OWASP (www.owasp.org) and others to ensure that the GLOPortal CMS is as secure as possible; it must be noted that no system can ever be "tamper" or "hack proof", this has been proven by the many successful attacks against some of the biggest online services in the world.
2. GLOvent takes appropriate measures to prevent and minimise risks of unauthorised access to, improper use and the inaccuracy of the customer's personal information. This includes, but is not limited to the following:
 - a. GLOvent will not disclose the customer's personal information to a person who is not directly involved in the delivery of our products/services without the customer's permission, unless compelled by law/in terms of a court order to do so, or in public interest or necessary to protect the rights and ensure the integrity and operation of its business and systems.
 - b. GLOvent uses enterprise standard technology such as MYSQL RDMS, Java Programming Language and Jboss Application Server. These technologies are tried and tested and used by a vast array of businesses around the world to create secure systems.

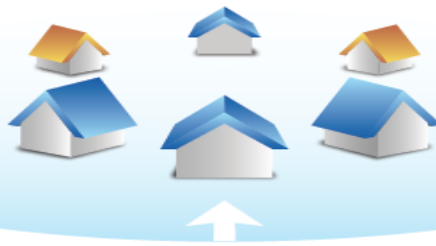


- c. GLOvent adheres to industry practices in terms of securing the server that the GLOPortal CMS is hosted upon, these practices include, but are not limited to, the use of Anti-Virus, RootKit Checking software, Secure Firewall Software and other best practice configuration standards that cannot be detailed as this would be counterproductive.
3. SSL (Secure Sockets Layer) is used by GLOvent to establish an encrypted link between the GLOPortal server and a web browser accessing the GLOPortal CMS. SSL is a connection standard security technology. (**see a copy of our SSL Security Certificate at the end of this document**).
4. The System and Data are hosted on our (GLOvent Solutions') dedicated server located at one of the leading Global Hosting Service Providers (Hetzner), the server is physically located in Cape Town, South Africa – all data is backed up daily to a separate server and the server runs a RAID system. Hetzner owns the hardware which GLO-Portal CMS operates upon and GLOvent leases this hardware from Hetzner; Hetzner at no point owns any data or software that resides on the server; a Key Clause from Hetzner's standard terms and conditions confirms this; this being "3.6. *We have no knowledge of, nor interest in Customer content hosted on your behalf by Hetzner on a Server or a shared hosting package. We also do not in any way contribute to or approve the content.*" For the full Hetzner terms and conditions, please visit their website at: <http://www.hetzner.co.za/legal>

On a **Commercial level**, the following is stated in the standard service agreement presented to all clients:

5. Data security (specifically the member database) is specifically detailed in the Service Agreement. It is stated that GLOvent is not allowed to use the database for any other purpose than for the fulfilment of their agreement and is not allowed to make know or disseminate the database or any part thereof to any third party. This includes service providers and sponsors if the sponsorship model is selected.
6. The Service Agreement also specifically notes that all data (including the member database, design elements, etc) remains the property of the client and that GLOvent is to return this data to the client at anytime if requested.

For more information on the GLOPortal Community Management System (CMS) or on GLOvent Solutions, please visit our website at www.glovent.co.za. GLOvent can also be contacted at info@glovent.co.za.



Verified

Secure Site by GoDaddy.com

This Web site is secured with a GoDaddy.com Web Server Certificate. Transactions on the site are protected with up to 256-bit Secure Sockets Layer encryption.

Domain Control Verified

GoDaddy.com has verified that the certificate holder controls the domain cms.gloportal.co.za.

Site Name

cms.gloportal.co.za

Certificate Status

Certificate is valid (3/9/15 1:50 PM to 3/9/16 9:43 PM).



Standard SSL

[GoDaddy Repository](#)