SimpleFund360

Automate your data collection with BGL Bank Data Service

Bank Data Service security & privacy

BGL takes security seriously and invests heavily to protect information. We view security as a continual improvement process and not just a once-off procedure.

1. Who is providing BGL Bank Data Service?

BGL has been providing software solutions to Accountants, Lawyers, Planners and Professional Firms for over 25 years and has been providing data services for over 5 years.

BGL's Simple Fund software is used to maintain over 75% of Australia's Self Managed Superannuation Funds. The economies of scale that BGL's service offers can make it easier for BGL to provide the highest levels of physical and digital security levels that most Accountants, Financial Planners and SMSF Administrators cannot implement on their own.

If the Bank Data is to be provided to BGL's Simple Fund 360 application, no other organisations apart from BGL are involved.

If the Bank Data is to be provided to BGL's Simple Fund software, BGL will use SISS Data Services Pty Ltd to securely transmit the data to Simple Fund located on a Practice's server.

SISS Data Services (SISS) is a software company specialising in data feed solutions for the accounting, software and financial services industry. SISS is a private, independently owned and operated company based in Australia.

2. Authority Forms

Each Bank Account holder must sign a Third Party Authorisation form which has been approved by the Bank. This forms part of the written agreement BGL has with each bank and is the only entity which is allowed to receive data directly from each Bank.

BGL will never ask for your Internet Banking user name or password and does not use any screen scraping technology. All data is received directly from each Bank via the Bank's prescribed channel.

Authority Forms returned to BGL's office are only handled by authorised staff members. Access to BGL's office is via security card only. All documents are shredded after use.

3. Is the Data Secure?

3.1 Banks to BGL

BGL complies with all the security requirements set by each of the individual Banks. Each Bank will send data to BGL on authorised accounts via a secure channel prescribed by each Bank. BGL can only receive historical information. BGL cannot transact on any bank account.

BGL's infrastructure and online software security is regularly reviewed by external specialists. This includes all critical risks contained in OWASP's top 10. BGL's Bank Data servers run a *NIX based operating system firewall and perimeter based security policies protected against unauthorized service access. Daily logging and monitoring of requests are performed to ensure that the connected internal clients are the authorized hosts.

3.2 BGL to SISS

BGL sends data to SISS via a Secure File Transfer Protocol (SFTP) using certificate based authentication. This is a one way transfer, with data push originating from BGL. SISS cannot request or access data from BGL's servers.

3.3 SISS to BGL Simple Fund (Practice)

All Data sent by SISS to BGL Simple Fund software is via an SSL web service (All data is encrypted) and requires a user name and password supplied to the Practice.

3.3 BGL Simple Fund 360

BGL's Simple Fund 360 application is signed by an SSL certificate meaning all data transferred between BGL and your Internet Browser is encrypted (the same as Internet Banking). Access is username and password protected and passwords resets are emailed to the user's email address. Users can only access information that they have permission to view. Access in Simple Fund 360 is role-based meaning that the Practice Administrator has complete control who can access your information. All Users have an audit trail which is logged including IP Address.

4. Where is the Data Stored?

Bank Data is and will always be stored in Australia. No Data will ever be transmitted overseas.

4.1 BGL's Data Centre

BGL's chosen Data Centre is located in Australia and isolated from BGL's own internal office networks. Only strictly controlled BGL staff with authorisation can remotely access the servers which house the data. BGL regularly review access control and when an employee no longer has a business need for these privileges, his or her access is immediately revoked.

The chosen Data Centre is state of the art, utilising innovative architectural and engineering approaches. The chosen Data Centre has many years of experience in designing, constructing, and operating large-scale data centres. This experience has been applied to the Hosting platform and infrastructure. The data centre is housed in nondescript facilities. Physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilising video surveillance, intrusion detection systems, and other electronic means.

Authorized staff must pass two-factor authentication a minimum of two times to access data centre floors. All visitors and contractors are required to present identification and are signed in and continually escorted by authorised staff. The Data Centre Host only provides data centre access and information to employees and contractors who have a legitimate business need for such privileges. When an employee no longer has a business need for these privileges, his or her access is immediately revoked, even if they continue to be an employee of the Hosted Data Centre. All physical access to data centres by the chosen Data Centre employees is logged and audited routinely.

4.2 BGL Data Centre - Storage Device Decommissioning

When a storage device has reached the end of its useful life, procedures include a decommissioning process that is designed to prevent customer data from being exposed to unauthorized individuals. The chosen data centre uses the techniques detailed in DoD 5220.22-M ("National Industrial Security Program Operating Manual ") or NIST 800-88 ("Guidelines for Media Sanitization") to destroy data as part of the decommissioning process. All decommissioned magnetic storage devices are degaussed and physically destroyed in accordance with industry-standard practices.

4.3 BGL Data Centre - Security Controls

The Data Centre built on an environment with extensive and validated security and controls, including:

- Service Organization Controls 1 (SOC 1) Type 2 report (formerly SAS 7011 Type II report), with periodic independent audits to confirm security features and controls that safeguard customer data.
- ISO 270001 Certification, an internationally-recognized security management standard that specifies leading practices and comprehensive security controls following the ISO 27002best practice guidelines.
- PCI DSS12Level 1 compliance, an independent validation of the platform for the secure use of processing, transmitting, and storing credit card data.
- Relevant government agency and public sector compliance qualifications, such as an ITAR-compliant environment.

4.4 SISS Data Services – Data Center

SISS Data Services hosts their data at Australia's BulletProof. BulletProof provides dedicated servers, fully managed application server and managed hosting offerings powered by Bulletproof Networks' Tier 1 infrastructure and support now power Mission Critical Hosting for some of the largest companies and carriers in Australia.

5. Privacy of my data

BGL treats all data with upmost privacy. BGL's privacy policy can be found at http://www.bglcorp.com/about-bgl/privacy-policy

SISS treats all data with upmost privacy. SISS's privacy policy can be found at https://sissdataservices.com.au/privacy-policy-2/