substance.

## Data Processing Statement

Substance has created this document to outline the processes we have implemented to comply with the new data protection legislation in the UK (the **GDPR**). The legislation will come into force on 25th May 2018.

This document is written for Views customers and users.

Substance is a data processor in respect of any personal data uploaded to Views by you or on your behalf. This means that we do not control the personal data that you have collected or decide what purpose to use it for.

You, as a customer or user of Views, will be the data controller of the personal data you upload to Views. This means that you owe certain obligations to the individuals whose personal data you hold.

Under the GDPR you are responsible for ensuring that you are legally entitled to process the personal data you store on Views and to authorise Substance to process such personal data on your behalf. You are also required to satisfy yourself that the security measures we have implemented are appropriate, taking into account the type of personal data you store on Views.

Further information regarding your obligations under the GDPR is available on the UK Information Commissioner's website – https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

If you would like to discuss this document or have any concerns regarding the processing of personal data on Views, please contact your Substance representative or email us at info@substance.net

substance.

# Views Data Security Statement

## 1.0 About us

Substance is the organisation behind Views. The company has been trading since November 2005 and launched Views in 2010. Substance is based in Manchester, UK.

## 2.0 Role

Under the GDPR, Substance is classified as a data processor in respect of any personal data stored on Views by you or on your behalf.

## 3.0 Accreditation

Substance is ISO27001 accredited and was first awarded the accreditation for data and information security and management in October 2010. Substance's most recent audit was conducted on 11 August 2017.

Internal data systems (both physical and online) are audited by an ISO27001 external evaluator on an annual basis to ensure continued compliance with the standard.

## 4.0 Hosting

The Views system is hosted live using Rackspace, a UK based virtual hosting company. Rackspace UK is located in Hayes, Middlesex.  The company's centres are accredited to ISO27001 standards.

## 5.0 Views "App" Backup policy

Databases are backed-up daily both locally and to a remote backup server and are encrypted using GPG with a 1024bit DSA keypair and 2048bit ELG-E key size. Local backups are kept for 2weeks and remote backups are held for 90 days. After these terms the expired backup files are securely wiped.
Back-ups are also securely copied over to the programme server nightly ready for statistical processing. Therefore, a total of three copies of the data are kept: one of the live server and two on back-ups. The code is held within a Subversion repository which is itself backed up in an alternate location.

## 6.0 Views "Programme" Backup policy

There are no database backups stored against the Programme server as data is rebuilt on a nightly basis from live data rendering any backup redundant. The code is held within a Subversion repository which is itself backed up in an alternate location.

## 7.0 Access Control - Physical Security

Physical access to the Views sever storage location is securely managed. Rackspace personnel are required to display their identity badges at all times when onsite at Rackspace Data centre and non-Data centre facilities. Two factor

authentication is used to gain access to sensitive areas of the Data centre facilities. Electromechanical locks are controlled by biometric authentication (e.g. 12 hand geometry scanner) and key-card/badge. CCTV surveillance has been installed at all entrance points on the interior and exterior of the buildings housing Data centres and is monitored by authorised Rackspace personnel.

## 8.0 Access control: User authentication

Access to Views is protected by a strong password enforcement policy with passwords including a mix of lower case, upper case, numerical, and symbol characters. Each password must have a minimum of 12 characters.

Views offers full control on access level via user groups, with each group having a defined level of access and functionality. This is managed by you depending on your internal security requirements.

You can also control access to individual data records via the systems 'Data Security' module.

## 9.0 Access control: administrator access

Administrative access to Views accounts is limited to Support Administrators and our team of developers. Access to customer data is granted to such personnel only with express permission from you (for instance, in the context of investigating a system bug or maintenance issue).

Access to the underlying operating systems of our servers is restricted to our Systems Administrator Team, who also have access to the backups for restoration purposes.

## 10.0 Data Downloads and Deletions

If you decide to close your Views account, you can request an export of your data stored on Views. We will provide the export in the format of a series of CSV tables which will be made available to authorised users via the Views platform. An authorised user will have 30 working days from receipt of download to export the data. After this time, we will securely delete all data stored on your Views account.

## 11.0 Change Log

The Views Database logs any changes (creation, edits and deletions) made to record. The Change Log tracks the time and date of change and identifies the user who made the change. The change log is accessible to authorised Substance employees and is retained for 30 days as standard practice. It is possible to request a variation to the standard retention policy at the initial contracting/negotiation stage. A change log can be made available to you via a nominated admin user upon request.

## 12.0 Maintenance and Support

substance.

Substance continuously monitors Views' data system security and has in place periodic server updates for critical security issues. Additionally, the Views system is monitored manually several times a day to check the site is operational and not experiencing excessive slow down due to volumes of traffic.

Substance uses cryptographic authentication for all systems administration. Access to servers are via SSH keys granted solely to server administrators.

Substance and any associated contractors keep and can provide audit trails of maintenance and support tasks should they be required.

## 13.0 Intrusion detection and prevention

Substance has a brute force login prevention process in place which locks out a user after five failed login attempts. Logs of unsuccessful login attempts are kept to monitor for automated attacks.

## 14.0 Penetration Testing

Penetration testing is a systematic process of probing for vulnerabilities in applications and networks. It is essentially a controlled form of hacking in which the 'attackers' operate on your behalf to find the sorts of weaknesses that criminals exploit.

The process of penetration testing involves assessing chosen systems for any potential weaknesses that could result from poor or improper system configuration, known and unknown hardware or software flaws, and operational weaknesses in process or technical countermeasures.

Substance has a policy to PEN test its Views platform on an annual basis and to address any vulnerabilities which are identified.

The last Views PEN test was undertaken in November 2017.

## 15.0 Business Continuity

The total time to reinstate the Views system if the case of complete system failure would be two days. Data can be restored within 4 hours.

In terms of a disaster recover strategy, Servers used by Substance are imaged, so that a new server can be created at short notice.  In the event of a complete system failure where the server image was also lost, Codebase would be restored from offsite SVN repo and data restored from remote backups.

The building in which the Views system is hosted are bomb resistant and fire resistant. Power supply is secured using UPS, back-up generators with separate power suppliers from separate grids. Should a total utility power outage ever occur, all of our data centres' power systems are designed to run uninterrupted, with every server receiving conditioned UPS (Uninterruptible Power Supply) power.

Our UPS power subsystem is N+1 redundant, with instantaneous failover if the primary UPS fails. If an extended utility power outage occurs, our routinely tested, on-site diesel generators can run indefinitely.

Substance does not make specific guarantees on up time. However, we do offer forward notice for any scheduled maintenance and downtime.

## 16.0 Hardware

The server used for Views is the x86_64 Virtual server

In the case of decommissioned servers, data is securely destroyed. Redundant servers are decommissioned in accordance with ISO27001 standard. All redundant portable media used by Substance for the Views system to host personal data will be destroyed (if appropriate) on the site to HMG IA standards. If the media is to be re-used, it will be sanitised by the contractor which employers ISO 9001:200 and Infosec 5 accredited processes. Redundant cloud servers from Rackspace are wiped by them to HMG IA standard.

## 17.0 Test Environment

The test environment used for the development of the Views system has a separate code area from live and does not share the same data as it is on a separate dedicated server.

No data is transferred from the development area to live. This action is only performed the other way around. Code is merged to the testing server, then live and only tested active code is moved to live.  All code changes are reviewed.

## 18.0 Incident Management

All staff and contractors for Substance have a responsibility for reporting information security incidents or breaches of information confidentiality using Substance's Security Incident and Corrective Action Report (SICAR) form.  Substance's Contracts Manager and one Director have to be informed.  When reporting an incident, all staff and contractors must ensure that sufficient information is entered into the SICAR to allow the incident to be investigated the root cause identified and wherever possible the risk of recurrence minimised or eliminated.

Substance will inform Views clients of any serious personal data breaches relating to them as soon as is practically possible, providing full details of the nature and extent of the breach.