SDV© platform

GDPR Statement

Prepared for: All clients

Prepared by: Xiatech Consulting Ltd

1st May 2018

Document Revision and Approvals:

V0.1	1st May 2018	First draft	Jonathan Summerfield, Kurt Maile, Simon Norris

Table of Contents

GDPR Statement for the Xiatech Single Data View Platform

Published: 23rd May 2018

This Statement forms part of the Master Services Agreement between Xiatech and its clients and is therefore intended to formalise the relationship with respect to the GDPR and the processing of sensitive data

1. Xiatech's Corporate Trust Commitment

Xiatech is committed to achieving and maintaining the trust of our customers. Integral to this mission is providing a robust security and privacy program that carefully considers data protection matters across our suite of services, including data submitted by our customers to our services ("Customer Data").

The General Data Protection Regulation (GDPR) is a comprehensive European privacy law that takes effect on May 25, 2018. Xiatech welcomes this law as an important step forward in streamlining data protection requirements across the European Union and as an opportunity for Xiatech to deepen our commitment to data protection.

1.1. Xiatech's GDPR Commitment

We are committed to our customers' success, including compliance with the GDPR.

Similar to existing privacy laws, compliance with the GDPR requires a partnership between Xiatech and our customers in their use of our services. Xiatech will comply with the GDPR in the delivery of our service to our customers. We are also dedicated to helping our customers comply with the GDPR. We have closely analysed the requirements of the GDPR, and are working to make enhancements to our products, contracts and documentation to support compliance with the GDPR.

2. Services Covered

This document describes our policies in relation to the architecture, security, privacy and administrative, technical and physical controls applicable to the services ("Covered Services") branded as the following:

- The Single Data View ("SDV") platform
- The Single Data View Integration Platform as a Service (IPAAS)
- The Single Data View Operational Data Store
- The Single Data View Reporting & Analytics
- The SDV Agent and SDV Controller

The Xiatech SDV will only collect data from our client systems under these Covered Services under the terms of the Master Services Agreement and associated Work Orders. Xiatech do not collect data from other sources unless instructed to do so under the agreed terms.

3. Architecture and Data Segregation

The Covered Services are operated in a multitenant architecture that is designed to segregate and restrict Customer Data access based on business needs. The architecture provides an effective logical data separation for different customers via customer-specific "Organization IDs" and allows the use of customer and user role-based access privileges. Additional data segregation is ensured by providing separate environments for different functions, especially for testing and production.

The specific infrastructure used to host Customer Data is described in Appendix A where the data is hosted on the infrastructure of a public cloud provider ("Public Cloud Infrastructure"). For customers who elect Public Cloud Infrastructure, this will mean the underlying physical infrastructure on which your Customer Data is stored will be with a public cloud provider for what is commonly referred to as

Infrastructure as a Service, and the Covered Services will run on top of the public cloud provider.

4. Xiatech as a Data Processor

Under the GDPR, there is a difference between a controller and a processor:

- A controller is a natural or legal person or organisation which determines the purposes and means of processing personal data; and
- A processor is a natural or legal person or organisation which processes personal data on behalf of a controller.

Under the terms of the SDV platform, Xiatech are considered a processor and our clients are considered the controllers.

4.1. Control of Processing

Under the terms of our Master Services Agreement, Xiatech undertake the following provisions in relation to our Clients' data:

- Only act and process data on the written instructions of the controller in relation to the provision of the Covered Services of the SDV
- Ensure that people processing the data are subject to a duty of confidence
- Take appropriate measures to ensure the security of processing
- Only engage sub-processors with the prior consent of the controller and under a written contract
- Assist the controller in providing subject access and allowing data subjects to exercise their rights under the GDPR
- Assist the controller in meeting its GDPR obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments
- Delete or return all personal data to the controller as requested at the end of the contract
- Submit to audits and inspections, provide the controller with whatever information it needs to ensure that they are both meeting their Article 28 obligations, and tell the controller immediately if it is asked to do something infringing the GDPR or other data protection law of the EU or a member state

Xiatech request that our SDV customers shall, in its use of the Covered Services, collect and process personal data in accordance with the requirements of Data Protection Laws and Regulations. For the avoidance of doubt, our customers' instructions for the processing of personal data shall comply with Data Protection Laws and Regulations. Our customers, as Data Controllers, shall have the sole responsibility for the accuracy, quality, and legality of personal data and the means by which the personal data was acquired.

Xiatech commit to treat personal data as confidential information and shall only process personal data on behalf of and in accordance with Customer's documented instructions for the following purposes: (i) processing in accordance with the SDV Master Services Agreement and applicable Work Order Form(s); (ii) processing initiated by our customers' users in their use of the Covered Services; and (iii) processing to comply with other documented reasonable instructions provided by our customers (e.g., via email) where such instructions are consistent with the terms of the Agreement.

4.2. Processor responsibilities

In addition, as responsibilities under the GDPR processor terms, Xiatech commit to:

- only act on the written instructions of the controller (Article 29)
- not use a sub-processor without the prior written authorisation of the controller (Article 28.2

- co-operate with supervisory authorities (such as the ICO) in accordance with Article 31
- ensure the security of its processing in accordance with Article 32
- keep records of its processing activities in accordance with Article 30.2
- notify any personal data breaches to the controller in accordance with Article 33
- employ a data protection officer if required in accordance with Article 37 and
- appoint (in writing) a representative within the European Union if required in accordance with Article 27

4.3. Third party functionality

As part of the SDV ecosystem, Xiatech use technologies from third parties to store, process and encrypt sensitive data. Although only Xiatech employees can access the underlying SDV services, Xiatech are obligated to inform our clients that we use such third parties, which can be viewed in Appendix A.

5. Privacy of Data

5.1. Customer Data

As a rule, we will never divulge your personal information to any Third Parties except:

- If we are under a duty to disclose or share your personal data in order to comply with any legal obligation
- If Xiatech Consulting Ltd or substantially all of its assets are acquired by a third party, in which case personal data held by it about its customers will be one of the transferred assets

5.2. Data Subject Requests

Xiatech shall, to the extent legally permitted, promptly notify our customers if Xiatech receives a request from a Data Subject to exercise the Data Subject's right of access, right to rectification, restriction of Processing, erasure (“right to be forgotten”), data portability, object to the Processing, or its right not to be subject to an automated individual decision making (“Data Subject Request”).

Taking into account the nature of the Processing, Xiatech shall assist our customers by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of our customers’ obligation to respond to a Data Subject Request under Data Protection Laws and Regulations.

In addition, to the extent our customers, in the use of the Covered Services, does not have the ability to address a Data Subject Request, Xiatech shall upon a customer’s request provide commercially reasonable efforts to assist our customers in responding to such Data Subject Request, to the extent Xiatech is legally permitted to do so and the response to such Data Subject Request is required under Data Protection Laws and Regulations. To the extent legally permitted, our customers shall be responsible for any costs arising from Xiatech’s provision of such assistance.

5.3. Return of Customer Data

Within 30 days post contract termination, customers may request return of their respective Customer Data submitted to the Covered Services (to the extent such data has not been deleted by Customer). Xiatech shall provide such Customer Data in an agreeable format.

5.4. Deletion of Customer Data

After termination of all subscriptions associated with an environment, Customer Data submitted to the Covered Services is retained in inactive status within the Covered Services for 120 days, after which it is securely overwritten or deleted from production within 90 days, and from backups within 180 days.

Without limiting the ability for customers to request return of their Customer Data submitted to the Covered Services, Xiatech reserves the right to reduce the number of days it retains such data after contract termination. Xiatech will update this SDV GDPR Documentation in the event of such a change.

Day 0, subscription terminates	Day 0 - 30	Day 30 - 120	Day 121 - 211	Day 121 - 301
	Data available for return to customer	Data inactive and no longer available	Data deleted or overwritten from production	Data deleted or overwritten from backups

6. Security Controls

6.1. Security access and transmission

- We are committed to ensuring that your information is secure. In order to prevent unauthorised access or disclosure, we have put in place suitable physical, electronic and managerial procedures to safeguard and secure the information we collect from your operational systems
- Unfortunately, the transmission of information via the internet is not completely secure. Although we will do our best to protect your personal data, we cannot guarantee the security of your data transmitted to our site; any transmission is at your own risk. Once we have received your information, we will use strict procedures and security features to try to prevent unauthorised access.

6.2. Security Policies and Procedures

The Covered Services are operated in accordance with the following policies & procedures to enhance security:

- User access log entries will be maintained, containing date, time, user ID, URL executed or entity ID operated on, operation performed (created, updated, deleted) and source IP address. Note that source IP address might not be available if NAT (Network Address Translation) or PAT (Port Address Translation) is used
- If there is suspicion of inappropriate access, Xiatech can provide customers log entry records and/or analysis of such records to assist in forensic analysis when available. This service will be provided to customers on a time and materials basis
- Passwords are not logged
- Certain administrative changes to the Covered Services (such as password changes and adding custom fields) are tracked and are available for viewing by a customer's system administrator
- Xiatech personnel will not set a defined password for a user. Passwords are reset to a random value (which must be changed on first use) and delivered automatically via email to the requesting user

6.3. Audits and Certification

The following security and privacy related audits and certifications are applicable to the Covered Services:

- **ISO 27001/27017/27018 certification**: Xiatech operates an information security management system (ISMS) for the Covered Services in accordance with the ISO 27001 international standard and aligned to ISO 27017 and ISO 27018. Xiatech are currently undergoing ISO 27001/27017/27018 certification for its ISMS from an independent third party. The Xiatech ISO 27001/27017/27018 Certificate and Statement of Applicability will be available upon request upon completion
- **Payment Card Industry (PCI)**: For the Covered Services Xiatech is not required to obtain compliance with the applicable Payment Card Industry Data Security Standard, as formulated by The Payment Card Industry Security Standards Council ("PCI DSS") as the SDV does not hold or process payment, credit card or similar data

6.4. Intrusion Detection

Xiatech, or an authorized third party, will monitor the Covered Services for unauthorized intrusions using network-based and/or host-based intrusion detection mechanisms. Xiatech may analyse data collected by users' web browsers (e.g., device type, screen resolution, time zone, operating system version, browser type and version, system fonts, installed browser plug-ins, enabled MIME types, etc.) for security purposes, including to detect compromised browsers, to prevent fraudulent authentications, and to ensure that the Covered Services function properly.

6.5. Security Logs

All systems used in the provision of the Covered Services, including firewalls, routers, network switches and operating systems, log information to their respective system log facility or a centralised syslog server (for network systems) in order to enable security reviews and analysis. These are provided by the third-party hosting partners listed in Appendix A.

6.6. Incident Management

Xiatech maintains security incident management policies and procedures. Xiatech notifies impacted customers without undue delay of any unauthorised disclosure of their respective Customer Data by Xiatech or its agents of which Xiatech becomes aware to the extent permitted by law.

Xiatech typically notifies customers of significant system incidents by email, and for incidents lasting more than one hour, may invite impacted customers to join a conference call about the incident and Xiatech’s response.

6.7. User Authentication

Access to Covered Services requires authentication via one of the supported mechanisms, including user ID/password, SAML based Federation, OAuth, Social Login, or Delegated Authentication as determined and controlled by the customer. Following successful authentication, a random session ID is generated and stored in the user's browser to preserve and track session state.

Xiatech shall ensure that Xiatech’s access to personal data is limited to those personnel performing services in accordance with the agreement of the Covered Services.

6.8. Data Protection Officer

Xiatech have appointed a data protection officer who can be reached at privacy@xiatech.co.uk

6.9. Physical Security

Production data centres used to provide the Covered Services are provided by our third-party providers listed in Appendix A. Xiatech are assured that these third parties have access control systems that permit only authorised personnel to have access to secure areas. These facilities are designed to withstand adverse weather and other reasonably predictable natural conditions, utilise redundant electrical and telecommunications systems, employ environmental systems that monitor temperature, humidity and other environmental conditions, and contain strategically placed heat, smoke and fire detection and suppression systems. Facilities are secured by around-the-clock guards, interior and exterior surveillance cameras, two-factor access screening and escort-controlled access. In the event of a power failure, uninterruptible power supply and continuous power supply solutions are used to provide power while transferring systems to on-site back-up generators.

6.10. Reliability and Backup

All networking components, network accelerators, load balancers, Web servers and application servers are configured in a redundant configuration. All Customer Data submitted to the Covered Services is stored on a primary database server with multiple active clusters for higher availability. All Customer Data submitted to the Covered Services is stored on a highly redundant disk storage and multiple data paths to ensure reliability and performance. All Customer Data submitted to the Covered Services, up to the last committed transaction, is automatically replicated on a near real-time basis to the secondary site and backed up to localised data stores by our third-party providers.

6.11. Disaster Recovery

Xiatech have selected third-party cloud providers to host the SDV platform and associated Customer Data. This is because these third-party production data centres are designed to mitigate the risk of single points of failure and provide a resilient environment to support service continuity and performance. The Covered Services utilise the third party secondary facilities that are geographically diverse from their primary data centres, along with required hardware, software, and Internet connectivity, in the event Xiatech production facilities at the primary data centres were to be rendered unavailable.

6.12. Viruses

The Covered Services do not scan for viruses that could be included in attachments or other Customer Data uploaded into the Covered Services by a customer. Uploaded attachments, however, are not executed in the Covered Services and therefore should not damage or compromise the Covered Services by virtue of containing a virus.

6.13. Data Encryption

The Covered Services use industry-accepted encryption products to protect Customer Data and communications during transmissions between a customer's network and the Covered Services, including through Transport Layer Encryption (TLS) leveraging at least 2048-bit RSA server certificates and 128-bit symmetric encryption keys at a minimum. Additionally, all data, including Customer Data, is transmitted between our third-party managed data centres for replication purposes across a dedicated, encrypted link utilising AES-256 encryption.

Appendix A

The list of third-parties that provide and host the Covered Services and components supplied as part of the SDV agreement are as follows:

- AWS hosted services – Lambda, DataBricks Spark, GoLang Microservices, Couchbase, API gateway, Kinesis Streams
- Google Cloud - Google BigQuery
- DevOps tooling – Cloudwatch, Hashicorp Terraform & Vault, Concourse
- Tableau Online, Tableau Server & Tableau Developer