Agnitio Rainmaker Security Statement

Any personal information you give to us will be processed in accordance with OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data", "EU Data Protection Directive (95/46/EC)" and "The Danish Act on Processing of Personal Data" (Act No. 429 of 31 May 2000, amended in July 2007).

Agnitio A/S strives to ensure that user data is kept securely, and that we collect only as much personal data as is required to provide our services to users in an efficient and effective manner. Agnitio Rainmaker suite uses some of the most advanced technology for internet security that is commercially available today. This Security Statement is aimed at being transparent about our security infrastructure and practices, to help reassure you that your data is appropriately protected. Agnitio maintains, and annually updates a general written Rainmaker Security Statement which details:

- System Continuity
- Human Resources Security
- Organizational Asset Control
- Access Control
- Physical and Environmental Security
- Data Security
- Operations Security
- Network Security
- System and Application Security
- Security Incident
- Data Protection

System Continuity

- **Redundancy:** Rainmaker architecture utilizes redundancy through the entire infrastructure, from load balancers, storage units and processing engines, to power.
- **Database Failover:** In the event of a planned or unplanned outage of our DB instance, it's automatically switched to a standby replica in another location within EEA. Failover times are typically 60-120 seconds.
- **Disaster Recovery Planning (DRP):** Agnitio has disaster recovery plans in place and tests them regularly in our testing environment on a bi-yearly basis.
- **Data Backup and Restoration**: Backups occur daily to a centralized backup system for storage in multiple geographically disparate sites. Backup activities are reviewed every day. Copies of backups are stored at a remote distance from the source systems and protected against unauthorized access and misuse. Retention period with 30 daily, 12 monthly, 5 yearly full backups on each instance.

Human Resources Security

- **Employee Screening:** Confidentiality and security is a serious concern for our clients and Agnitio employees are required to undergo background checks and provide specific documents verifying identity at the time of employment.
- **Confidentiality:** Every Agnitio employee must sign Group IT Policy that binds them to the terms of our data confidentiality policies to exercise complete confidentiality regarding all information relating to the company, its customers and other business partners.
- **Security Awareness /Training:** General information security training is provided to all new employees (both full time and temporary) as part of their onboarding. An annual security and privacy training requirement ensures employees refresh their knowledge and understanding. Development, Professional Services, IT Operations and Support staff receive further training specific to product development, and management of secure applications. Additional security training is also provided to employees who handle client sensitive data.
- **Termination of Employment:** Access to all the IT facilities is revoked at termination of employment.

Organizational Asset Control

- **Employee Workstations, Laptops, & Mobile Devices:** All laptops and workstations are secured and centrally managed. We diligently apply updates to employee machines and monitor employee workstations for malware. We also have the ability to apply critical patches and remotely wipe a machine.
- **Acceptable Use of Assets:** Acceptable Use of IT facilities and equipment are defined in Group IT Policy in the Agnitio Employee Handbook. Agnitio employees & contractors are required to sign off.
- **Data Storage Media Protection:** Agnitio Group IT Policy prohibits copying client data on removable media device, including flash drives, hard drives, tapes or other media, other than for legitimate business purposes and with the express authorization from the client.

Access Control

- **Access to Client Data:** Access to client data is limited to legitimate business need, including activities required to support clients' use of Rainmaker. Employees are given appropriate accounts on systems which they are authorized to access following the "least privilege" principle and may only access resources relevant to their work duties. Hosting providers have access to the facility hosting the infrastructure, and may provide remote-hand service for hardware maintenance under Agnitio supervision, but they do not have direct access to client data.
- **Admin Account Management:** Administrative access to Rainmaker resources is limited to IT Operations personnel and authentication requires public-key-based cryptography instead of password-based authentication. All other access to Rainmaker resources must be submitted by the requestor's manager. After review and approval, the request is logged for implementation. No login for general purpose administrative accounts exists. Granting access to IT system users is based on the principle of least privilege. In the case of Rainmaker, however, enforcement of least privilege is accomplished by granting ad-hoc access rights to Rainmaker, rather than granting access based on predefined roles.

- **User Account Management:** User accounts have unique usernames and passwords that must be entered each time a user logs on by default**.**
- **Remote Access:** Based on the sensitivity of data processed in Rainmaker suite, remote access to the servers of Rainmaker suite is not be permitted from outside Agnitio HQ network. VPN access requires user account and sufficient permission on Agnitio Active Directory system. VPN access is logged on the server for 30 days and for 5 years at remote backup site. SSH/RDP access to the system is managed at gateway level, allowing only Agnitio IP addresses. Remote access to the production servers is limited to IT Operations team. In the case other staff requires access to the production servers, remote access is granted for limited period by the IT Operations team.
- **Password Management:** User application passwords have minimum complexity requirements (no less than 8 characters with at least 1 uppercase, 1 lower-case and 1 digit). Once the user has created a password hashes are stored in the DB. It is not possible to retrieve the original password. Admin password complexity rules are enforced in all environments to protect against brute force dictionary or other passwords threats. Shared credentials are not allowed in production environment. Password are hashed and salted with a long hash algorithm. Two factors authentication is enforced for administration access.

Data Security

- **Data Classification:** All data collected by Agnitio on behalf of its clients for Rainmaker is the property of the respective clients and classified as either “Sensitive Data”, “Personal Dara” or “Confidential Data” under Rainmaker Data Classification Guideline, which provides employees with the necessary guidance for the handling of all information according to its classification. Data classification is carried out whenever a new data processing system or project is proposed, or when revision to existing data practices are planned.

- **Data Life Cycle Management:** We are committed to industry best practice when it comes to prevent loss, misuse, alteration, unauthorized access, unlawful or unnecessary processing of the information we collect throughout data’s life cycle from collection and initial storage to the time when it becomes obsolete and is destroyed. The life cycle includes five phases. Appropriate measures are deployed to properly protect the data at each phase:

    - **Collection/Creation:** It applies to colleting, creating or changing a data or content element. Creation is the generation of new contents or the alternation/updating of existing content, either structured or unstructured:
        - ✓ Assign proper data classification to the data.
        - ✓ Specify necessary security measures for the data, commensurate with the data classification as well as other contractual or legal requirements.
        - ✓ Determine whether classification marking is needed.
        - ✓ Determine the retention period for the data.

    - **Use**: it refers to the stage when the user is interacting with the data.
        - ✓ Apply need-to-know and least privilege principles when need to access the data.
        - ✓ Encrypt classified information when transmitted over un-trusted network (e.g. internet).

- ✓ Monitor for possible vulnerabilities and attacks.

- **Disclosure/Share:** it refers to the stage when exchanging data with users or external
  - ✓ Apply need-to-know and least privilege principles when need to access the data.
  - ✓ Encrypt classified information when transmitted over un-trusted network (e.g. internet).
  - ✓ Monitor for possible vulnerabilities and attacks.

- **Storage / Retention**: it's a process of transferring data from active use into long-term storage. A combination of encryption and asset management is used to protect the data and ensure its availability.
  - ✓ Do not store classified information in privately-owned computer resources.
  - ✓ Encrypt classified information during storage.
  - ✓ Limit access to the systems on which data is stored.
  - ✓ Maintain a record of repositories where classified information is being stored.

- **Destruction:** When the data is no longer needed, it should be permanently destructed. Verification is done to ensure the data in all active storage or archives has been destructed.
  - ✓ Perform proper data sanitization / disposal on devices storing classified data designed to prevent customer data from being exposed to unauthorized individuals. Our service provider uses the techniques detailed in DoD 5220.22-M or NIST 800-88 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.

- **Data Encryption:** Rainmaker uses encryption to protect the data and enforce confidentiality during transmission and storage:
  - **SSL/TLS Encryption (SHA256 hash algorithm):** All communications with Rainmaker suite are sent over SSL/TLS that is designed to protect against eavesdropping, tampering, and message forgery. This ensures that user data in transit is safe, secure, and available only to intended recipients.
  - **Storage Encryption:** Storage volumes and backup data are encrypted with 256-bit Advanced Encryption Standard (AEC-256).

- **Storage Device Decommissioning:** When a storage device has reached the end of its useful life, the procedures include a decommissioning process that is designed to prevent customer data from being exposed to unauthorized individuals. Our service provider uses the techniques detailed in DoD 5220.22-M or NIST 800-88 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.

Physical and Environmental Security

- **Data Center Security:** Rainmaker employs a hybrid cloud development model with virtualized resources. The infrastructure is divided into multiple, geographically dispersed colocation facilities. These facilities are located in Dublin, Ireland and London, United Kingdom.

All data centers have obtained a SOC (Service Organization Control) report or ISO 27001 certification, and employ industry best-practices, including badge and biometric access entry systems, redundant power sources, redundant air conditioning units and fire suppression systems. Security personnel and cameras monitor these locations 24 hours a day, 365 days a year. Only authorized personnel are allowed inside any data center and all accesses are logged.

Operations Security

- **Segregation of Duties:** Only authorized personnel can administer systems or perform security management and operational functions. Authorization for and implementation of changes are segregated responsibilities wherever appropriate to the organization.
- **Software and Patch Management:** Latest security patches are applied to all operating system and application files to mitigate newly discovered vulnerabilities. Agnitio deploys security patches released by the vendors as necessary to development, testing, and production systems after validation in testing environment. We deploy software that has been made publicly available through the OS vendor and software that has been developed by us internally which meet the business' specific needs and requirements. All other software is tested and examined locally and in QA environment prior to considering its use in production to avoid undesired effects.
- **Protection against Malware**: All Windows production external-facing web servers have anti-malware software installed and are scanned daily; and all deploy code is scanned for malware. None of Linux production servers are exposed directly to the internet. Strict rules are configured in firewall and only authorized personnel are allowed to access from specific IPs. Furthermore, Agnitio utilizes the controls, which most likely protect against virus and malware intrusion such as: principle of least privilege, applying security patches regularly, prohibiting remote root login, firewall, isolating the applications in private subnet, using software only from trusted sources.
- **Security Surveillance:** Agnitio uses an industry standard enterprise application management solution to monitor systems 24/7, trigger alerts based on event logs, and to facilitate alerting, trend analysis, and risk assessment. Escalation procedures exist to ensure the timely communication of significant security incidents through the management chain and ultimately to any affected client.
- **Logging:** All events and logs from applications and systems are managed in central log server in one place. The logs contain information on when data is entered, changed, removed or altered and by whom. Activity logs are stored in the database as well as available on UI (Mobilizer) for a person who has right permissions. He/she is able to view what activity was done, when it was done, who did and from which hostname (IP address). Database access is limited to IT Operations team.
- **Data Backup and Restoration:** Backups occur daily to a centralized backup system for storage in multiple geographically disparate sites. Backup activities are reviewed every day. Copies of backups are stored at a remote distance from the source systems and protected against unauthorized access and misuse. Retention period with 30 daily, 12 monthly, 5 yearly full backups are made on each instance.
- **Technical Vulnerability Management:** Agnitio runs a bi-yearly security scan of the production environment and contracts annually with a reputable third party security firm to conduct a comprehensive application penetration test and network vulnerability scan of Rainmaker. The primary objective of these scans and tests is to gain independent third-party validation of security stance and provide actionable recommendations for mitigation of any risks that may have been identified. All critical

issues confirmed are remediated immediately. Issues of lesser severity are evaluated for resolution as part of the standard release process.

Network Security

- **Network Isolation:** Production servers are isolated in virtual private environment. Firewall filters are present on both ingress and egress traffic.
- **Traffic restriction:** Traffic is restricted by any IP protocol, by service port, as well as source/destination IP address (individual IP or Classless Inter-Domain Routing (CIDR) block). Agnitio maintains a default-deny-all policy. All unused ports on the production network are disabled to prevent packet sniffing by unauthorized devices.
- **Remote Access:** Based on the sensitivity and confidentiality of data processed in Rainmaker suite, administrative access to the production network is only permitted from Agnitio HQ network where access controls are provided by Agnitio corporate Active Directory service.

System and Application Security

- **Production environment**: Agnitio employs a public cloud development model using both physical and virtualized resources for Rainmaker suite (Mobilizer, Engager, Sharedoc™). Rainmaker introduces multi-tenant and logical access controls using authentication and roles ensure the necessary separation between data from different clients and clients are provided with functionality to manage their own users and roles at the application level. The development and testing environments are isolated from the production.
- **Platforms:** Rainmaker uses a mix of Microsoft Windows and Linux virtualized servers as platforms for its proprietary data collection, content, and data processing and reporting applications.
- **Secure Coding Practices:** Our engineers use best practices and industry-standard secure coding guidelines to ensure secure coding.
- **Software Quality Assurance (SQA) Testing:** System functionality and design changes are verified in an isolated test SQA environment and subject to functional and security testing prior to deployment to active production systems. Use of test data extracted from production is not permitted.
- **Release Management:** All deployments into production or change to the production environment (new release, bug fix etc.) must be submitted to, reviewed and approved by the release management team prior to implementation. Both scheduled and emergency changes are tested in separate environments, reviewed and approved before deployment to the production environment.
- **Change Management**: Agnitio maintains and follows formal change management processes. All changes to the production environment (network, systems, platform, application, configuration, including physical changes such as equipment moves) are tracked and implemented by the IT Operations team. For any software release or change to take place there must be a rollback plan in place. Changes are tested in QA environment, QA team has to approve the changes before they are implemented.
- **Privacy Impact Assessment (PIA):** In order to reduce the risk of processing personal data, we perform PIA as a part of Feature Request process whenever a new data processing system or project is proposed, or when revisions to existing data practices are planned. Likelihood and severity of the

potential consequences, the sensitivity of the personal data, the number of data subject that could be affected by a potential breach are evaluated from both technical and compliance perspectives.

- **Application Access Security**: Mobilizer (the central component of Rainmaker suite) introduces a highly dynamic access control layer. Each content item (and most other entities) is only created in one organization in the application and it can never be made available to users belonging to other organizations. However inside any organization it is possible to create multiple access rules that grant users access to specific content items, usually based on some metadata matching between given user and content item. As conditions for those access rules are based on hierarchical metadata categories and both of these can be at any point altered, this results in a very dynamic and granular access control system.
- **Virtualization Security:** Different instances run on the same physical machine and are isolated from each other via the Xen hypervisor. In addition, the firewall resides within the hypervisor layer, between the physical network interface and the instance's virtual interface. All packets must pass through this layer, thus an instance’s neighbors have no more access to that instance than any other host on the Internet and can be treated as if they are on separate physical hosts. The physical RAM is separated using similar mechanisms. Customer instances have no access to raw disk devices, but instead are presented with virtualized disks. The disk virtualization layer automatically resets every block of storage used by the customer, so that one customer’s data is never unintentionally exposed to another. In addition, memory allocated to guests is scrubbed (set to zero) by the hypervisor when it is unallocated to a guest. The memory is not returned to the pool of free memory available for new allocations until the memory scrubbing is complete)

Supplier Relationship

- **Service Providers Screening:** We select and monitor outsourced providers in compliance with laws in the country where the data is processed, stored, and transmitted.
- **Non-disclosure Agreement:** We bind our service providers under contract to appropriate confidentiality obligations if they deal with any data.

Security Incident

- **Incident Handling Process:** Security incidents are escalated from the initial responders to Agnitio Customer Support team and the IT Operations team for client notification. Customer Support team will notify customer contacts assigned to the account as soon as possible after confirming them as being affected by a security or privacy breach, but in any event within 24 hours for significant events and within 2 business days for non-critical events.
- **Handling of personal data breach**: If Agnitio becomes aware of either (a) any unlawful access to any personal data on our equipment or in facilities; or (b) any unauthorized access to such equipment or facilities, where in either case such access results in loss, disclosure, or alteration of personal, Agnitio will promptly: (a) notify the Data Controller of the security incident without undue delay; and (b) take reasonable steps to mitigate the effects and to minimize any damage resulting from the security incident.

The notification will contain: the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of data records concerned, the likely consequences of the personal data breach, and the contact point where more information can be obtained, and the measures taken.

An unsuccessful personal data breach will not be subject to this. An unsuccessful personal data breach is one that results in no unauthorized access to personal data or to any our equipment or facilities storing personal, and may include, without limitation, pings and other broadcast attacks on firewalls or edge servers, port scans, unsuccessful log-on attempts, denial of service attacks, packet sniffing (or other unauthorized access to traffic data that does not result in access beyond IP addresses or headers) or similar incidents.

Data Protection

- **Data Processing Agreement:** Agnitio provides a data processing agreement to help customers meet their data protection obligations.
- **Data Transfer**: All client data is stored on the servers located within EEA (Ireland and United Kingdom). Data is neither transferred nor replicated outside of the data centers located in EEA.
- **Data Retention**: Personal data should not be kept (in an identifiable form) for longer than is necessary for the purposes for which the personal data was collected or further processed.
- **Data Correction and Deletion:** Personal data is corrected /deleted upon the data subject's request by Agnitio Support (support@agnitio.com) which will respond within 24 business hours for free of charge.
- **Privacy by Design (PbD) principles:** Agnitio takes the Privacy by Design (PbD) approach which is characterized by proactive rather than reactive measures. It anticipates and prevents privacy invasive events before they happen. We will review our practices regularly to ensure we are keeping the principles such as:

    - Enable the user to make informed decisions about sharing their personal information with a service.
    - Enable the user to make decisions at the appropriate time with the correct contextual information.
    - When learning user privacy decisions and providing defaults, allow the user to easily view and change their previous decisions.
    - Focus on usability and avoid needless prompting.
    - Active consent should be freely given, for specific data, and be informed.
    - Be clear and transparent to users regarding potential privacy concerns.
    - Be clear as to whether information is needed on a one-time basis or is necessary for a period of time and for how long.
    - Request the minimum number of data items at the minimum level of detail needed to provide a service.
    - Retain the minimum amount of data at the minimum level of detail for the minimum amount of time needed.
    - Consider potential misuses of retained data and possible countermeasures.
    - Maintain the confidentiality of user data in transmission, using HTTPS for transport rather than HTTP.
    - Maintain the confidentiality of user data in storage.
    - Control and log access to data

Contact

Please send any questions regarding this statement to privacy@agnitio.com. (Kensuke Lohse-Kimura, Security and Privacy Advisor)

Last updated: May 2016