**AUTOMATED TESTING (SPOT QA / VIRTUOSO "SpotQA"): SUB-PROCESSORS AND SECURITY MEASURES**

**1. SUB-PROCESSOR DETAILS (Processing Unit4 Customer Data)**

| Name of Sub-processor & DPO Details | Data Subject Type | Categories of Personal Data | Purpose of Processing | Countries where Processed |
|---|---|---|---|---|
| AWS Europe | Customer Data | Categories as set out in the relevant section of the Unit4 Details of Processing. | Hosting; Storage | Europe (Ireland) |

2. **TECHNICAL AND ORGANISATIONAL MEASURES**

("**Platform**" means https://app.virtuoso.qa)

SpotQA has implemented and will maintain the following security measures:

2.1. The following specific safeguards are made for SpotQA's technical security:

2.1.1. The Platform enforces user authentication at the application level through secure user/password combinations, supplemented by multi-factor authentication (MFA) where applicable.

2.1.2. Regular monitoring for vulnerabilities and any discovered vulnerabilities to be promptly addressed within defined time frames based on their severity, following a risk-based approach.

2.1.3. Encryption of Customer Data while at rest and in transit consistent with industry standards and at a minimum of 256-bit encryption.

2.1.4. Data redundancy and recovery plans, including at least daily backups of Customer Data, ensure timely recovery of the Platform in the event of a major incident.

2.1.5. SpotQA maintains network security with industry-standard techniques, including firewalls, intrusion detection, and prevention systems.

2.1.6. SpotQA uses the latest antivirus and malware protection software across all relevant systems, with regular monitoring and scanning to detect potential threats. Exceptions, where installing antivirus software may impact operation, performance or productivity, rely on inherent security measures that are designed to effectively prevent malware infections. This is monitored and maintained to ensure equivalent security effectiveness.

2.1.7. All Platform activity (including database activity) is logged for accountability,

2.1.8. Record and retain audit-logging information for all systems that handle confidential information, accept network connections, or make access control (authentication and authorisation) decisions.

2.1.9. Regularly conduct internal security audits and no less than annual external security assessments and penetration tests of company systems.

2.1.10. Maintains a digital record of personal data storage locations and follows a standard procedure for secure data deletion in compliance with applicable retention and deletion policies.

2.1.11. Ensures that Sub-processors implement robust technical and organisational measures to meet the requirements of the Applicable Data Protection Law, including data protection principles and security safeguards

2.2. The following specific safeguards are made for SpotQA's organisational security:

2.2.1. All employees are required to sign a confidentiality agreement when accepting a new hire offer and contractors who access the facilities and/or data required to sign a confidentiality or non-disclosure agreement.

2.2.2. All employees, contractors, and third-party users are assigned unique User-IDs and regularly briefed and trained on their information security roles and responsibilities, particularly in relation to their data protection obligations and Applicable Data Protection Law.

2.2.3. User administration procedures define user roles and privileges, access granting, changes, and termination, as well as ensuring appropriate segregation of duties and monitoring of activities.

2.2.4. Access rights are granted based on the 'least privilege' principle, with periodic reviews conducted to ensure that access remains appropriate for each user's role and responsibilities.

2.2.5. Upon termination of any employee/contractor, employee's/contractor's access to Customer Data on SpotQA's systems will be immediately revoked.

SpotQA shall implement the following additional measures for data minimisation (summarised below):

| Phase | Typical Duration | PII Location |
|---|---|---|
| **1. Environment Prep** | Hours-Days | Unit4 |
| **2. Data Loading** | Minutes-Hours | Platform (begins) |
| **3. Test Execution** | Minutes-Hours | Platform (active) |
| **4. Artifact Export** | Minutes | Both locations |
| **5. Data Purge Trigger** | Minutes | Unit4 |
| Duration for which PII hosted on Platform Platform* | Mins - 2 days | Unit4 Controlled |

* Time to complete data purge depends on the test execution volume.

Minimal Time Exposure: Five-Layer Temporal Defence

1. On-Demand Fetching: PII data is never pre-loaded or cached. Instead, the system employs an API call at test initiation to retrieve only relevant test data. This ensures PII exists in the Platform only during active test execution and review.
2. Ephemeral Storage Architecture: The SpotQA (Virtuoso) Test Execution Engine uses an ephemeral data store designed to hold PII exclusively during test execution and test execution review only.
3. Secure Results Transfer: Immediately upon test completion, execution results including screenshots and detailed reports are securely extracted by Unit4 and transferred to Unit4 via encrypted TLS connection. This critical step occurs before any data deletion, ensuring Unit4 receives complete test evidence and traceability while the test data remains temporarily intact for validation purposes.
4. Immediate Purge of data: Following successful results extraction, Unit4 triggers the purge to delete all fetched test data. Once Unit4 is satisfied with the extracted report they will trigger the purge. Time to complete the purge is dependent on the volume of test execution data entered by Unit4.
5. Fail-Safe Scheduled Purge: A redundant periodic purge provides double-safety by catching any residual data that might escape the primary purge controlled by Unit4. This defence-in-depth approach ensures even edge-case failures result in data removal within hours, not days.