SECURITY & PRIVACY SUMMARY

(last updated May 4, 2018)

Reflektive's Commitment to Security & Privacy

Reflektive is committed to achieving and preserving the trust of our customers, by providing a comprehensive security and privacy program that carefully considers data protection matters across our products and services, including data submitted by customers to our online service ("Client Data").

Covered Services

This documentation describes the security-related and privacy-related audits and certification received for, and the administrative, technical, and physical controls applicable to, the Reflektive Employee Performance Management Platform ("Service").

Architecture, Data Segregation, and Data Processing

The Service is operated in a multitenant architecture that is designed to segregate and restrict Client Data access based on business needs. The Reflektive 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, such as for testing and production.

Reflektive has implemented procedures designed to ensure that Client Data is processed only as instructed by the customer, throughout the entire chain of processing activities by Reflektive and its sub-processors.

Information Security Management Program ("ISMP")

Reflektive maintains a comprehensive information security management program that contains administrative, technical, and physical safeguards that are appropriate to (a) the size, scope and type of Reflektive's business; (b) the amount of resources available to Reflektive; (c) the type of information that Reflektive will store and process; and (d) the need for security and protection from unauthorized disclosure of such Client Data. The ISMP is documented and updated based on changes in legal and regulatory requirements related to privacy and data security practices and industry standards applicable to the Service.

Reflektive's ISMP is designed to:

- Protect the security, availability, and confidentiality of Client Data in Reflektive's possession or control;
- Protect against any anticipated threats or hazards to the security, availability, and confidentiality of Client Data by Reflektive or its agents;
- Protect against unauthorized access, use, alteration, or destruction of Client Data;
- Protect against accidental loss or destruction of, or damage to, Client Data; and
- Safeguard Client Data as set forth in any local, state or federal regulations by which Reflektive may be regulated.

1. Security Standards.

Reflektive's ISMP includes adherence to and regular testing of the key controls, systems and procedures of its ISMP to validate that they are properly implemented and effective in addressing the threats and risks identified. Such testing includes:

- Internal risk assessments;
- SOC2 (or successor standard) audits annually performed by accredited third-party auditors ("Audit Report").
- US/EU Privacy Shield certification annually renewed with the US Department of Commerce.

2. Security Audit Report.

Reflektive makes its most recent Audit Report available to its customers, and may provide a copy of Reflektive's then-current Audit Report upon request.

3. Assigned Security Responsibility.

Reflektive assigns responsibility for the development, implementation, and maintenance of its Information Security Management Program, including:

- Designating a Chief Information Security Officer and Chief Privacy Officer with overall responsibility; and
- Defining security and privacy roles and responsibilities for individuals with security and privacy responsibilities.

4. Relationship with Sub-Processors.

Reflektive conducts reasonable due diligence and security assessments of sub-processors engaged by Reflektive in the storing and/or processing of Client Data ("Sub-Processors"), and enters into agreements with Sub-Processors that contain provisions similar or more stringent than those provided for in this security and privacy documentation.

5. Background Check.

Reflektive performs background checks on employees who perform material aspects of the Service or may have access to Client Data.

6. Security Policy, Confidentiality.

Reflektive maintains an internal written Information Security Policy ("ISP") outlining the framework for management of Reflektive's information security. Reflektive requires all employees to acknowledge in writing, that they will comply with the ISP and protect Client Data at all times.

7. Security Awareness and Training.

Reflektive has mandatory security awareness and training programs for all Reflektive employees with respect to the implementation of and compliance with the ISP.

8. Disciplinary Policy and Process.

Reflektive maintains a disciplinary policy and process in the event Reflektive employees violate the ISP.

9. Access Controls.

Reflektive maintains policies and procedures, and has in place logical controls that are designed:

- To limit access to its information systems and the facility or facilities in which they are housed to properly authorized persons;
- To prevent personnel and others who should not have access from obtaining access; and
- To remove access in a timely basis in the event of a change in job responsibilities or job status.

Reflektive institutes:

- Controls to ensure that only those Reflektive personnel with an actual need-to-know will have access to any Client Data;
- Controls to ensure that all Reflektive personnel who are granted access to any Client Data are based on least-privilege principles;
- Periodic (no less than semi-annually) access reviews to ensure that only those Reflektive personnel with access to Client Data still require it.

10. Physical and Environmental Security.

Reflektive leverages Infrastructure-as-a-Service (IaaS) provider's controls that provide reasonable assurance that access to physical servers at the production data center is limited to properly-authorized individuals and that environmental controls are established to detect, prevent, and control destruction due to environmental extremes. These controls include:

- Logging and monitoring of unauthorized access attempts to the data center by the data center security personnel;
- Camera surveillance systems at critical internal and external entry points to the data center;
- Systems that monitor and control the air temperature and humidity at appropriate levels for the computing equipment; and
- Uninterruptible Power Supply (UPS) modules and backup generators that provide back-up power in the event of an electrical failure.

11. Data Encryption.

Encryption of Transmitted Data: Reflektive uses Internet-industry-standard secure encryption methods designed to encrypt communications between its server(s) and the customer browser(s), and between its servers and customer's server(s).

Encryption of At-Rest Data: Reflektive uses Internet-industry standard secure encryption methods designed to protect stored Client Data at rest.

12. Disaster Recovery.

Reflektive maintains policies and procedures for responding to an emergency or a force majeure event that could affect Client Data or production systems that contain Client Data. Such procedures include:

- Data Restoration: A procedure for restoring data from backup and restore services to meet the Recovery Point Objective described below;
- Disaster Recovery: A formal disaster recovery plan for the production environment designed to minimize disruption to the Service, which includes requirements for the disaster plan to be tested on a regular basis, currently four times a year;
- RPO / RTO: Recovery Point Objective is within the past 24 hours and a Recovery Time Objective to meet 99% uptime.

13. Secure Development Practices.

Reflektive follows secure application development policies, procedures, and standards that are aligned to industry-standard practices, such as the OWASP Top 10.

14. Malware Control.

Reflektive employs antivirus software on all company endpoints.

15. Data Integrity and Management.

Reflektive maintains security measures that ensure the following:

- Segregation of Data: The Service includes logical controls, including encryption, to segregate each customer's Client Data from that of other customers; and
- Back Up: Reflektive performs full backups of the database(s) containing Client Data on a daily basis.

16. Vulnerability Management.

Reflektive maintains security measures to monitor the network and production systems, including error logs on servers, disks and security events for any potential problems. Such measures include:

- Infrastructure Scans: Reflektive monitors alerts from intrusion-detection/intrusion-prevention tools, file-integrity monitoring systems, and detection of unauthorized wireless access points.
- Application Scans: Reflektive performs weekly application vulnerability scans. Vulnerabilities are remediated on a risk basis;
- External Application Penetration Tests: Reflektive engages third parties to perform application penetration testing on an annual basis.

17. Change and Configuration Management.

Reflektive maintains policies and procedures for managing changes to production systems, applications, and databases. Such policies and procedures include:

- A process for documenting, testing and approving the promotion of changes into production; and
- Platform-as-a-Service (PaaS) provider manages security patching process that requires patching systems in a timely manner based on a risk analysis.

18. Secure Deletion.

Reflektive maintains policies and procedures regarding the deletion of Client Data in compliance with applicable data protection laws, taking into account available technology so that Client Data cannot be practicably read or reconstructed.

19. Incident Management.

Reflektive maintains a security incident response plan that includes procedures to be followed in the event of an unauthorized disclosure of Client Data. The procedures in Reflektive's security incident response plan include:

- Roles and responsibilities: formation of an internal incident response team with a response leader;
- Investigation: assessing the risk the incident poses and determining who may be affected;

- Communication: internal reporting as well as a notification process in the event of a Security Breach;
- Recordkeeping: keeping a record of what was done and by whom to help in subsequent analyses; and
- Audit: conducting and documenting a root cause analysis and remediation plan.

Reflektive publishes system status information on the Reflektive Status website, at http://status.reflektive.com/. Reflektive typically notifies customers of significant system incidents by email to the listed admin contact and followed up with a call.

21. Security Breach Management.

- Notification: In the event of a Security Breach, Reflektive notifies impacted customers of such Security Breach. Reflektive cooperates with an impacted customer’s reasonable request for information regarding such Security Breach, and Reflektive provides regular updates on any such Security Breach and the investigative action and corrective action(s) taken.
- Remediation: In the event of a Security Breach, Reflektive, at its own expense, (i) investigates the actual or suspected Security Breach, (ii) provides any affected customer with a remediation plan, to address the Security Breach and to mitigate the incident and reasonably prevent any further incidents, (iii) remediates the effects of the Security Breach in accordance with such remediation plan, and (iv) reasonably cooperates with any affected customer and any law enforcement or regulatory official investigating such Security Breach.
- Unsuccessful Security Incidents: An unsuccessful Security Incident will not be subject to this Section 21. An unsuccessful Security Incident is one that results in no unauthorised access to Client Data or to any of Reflektive’s equipment or facilities storing Client Data, 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 unauthorised access to traffic data that does not result in access beyond headers) or similar incidents.