Impartner Technical and Organisational Security Measures

Effective Date: November 1, 2022

1. ENCRYPTION OF PERSONAL DATA

All data, including personal data, is encrypted in transit using TLS v1.2 or better encryption technology. Only industry-recognized TLS versions and ciphers are used. All data, including personal data, is encrypted at rest using AES-256 or better encryption technology.

2. CONFIDENTIALITY AND INTEGRITY

To ensure the confidentiality and integrity of data, Impartner employs the following measures:

2.1 Access control. Client data is housed in third-party data centers. All data centers have perimeter fences, biometric access controls, CCTV, full time guards, and user access auditing. Corporate offices have card readers at each door.

2.2 System access control. Access to data processing systems is only granted to authenticated users based on a role-based authorization matrix using the following measures: unique username & password assignment (at least 8 characters, regularly automatic expiration), intrusion detection systems and intrusion-prevention systems, regularly updated antivirus and spyware filters in the network and on the individual PCs and servers.

2.3 Data access control. Impartner will maintain administrative, physical, and technical safeguards for the protection, security, confidentiality and integrity of personal data processed by the Services, as described in the security documentation. Internally, the provisioning process requires manager approval prior to users being granted access to Impartner applications. Access revocation is conducted upon termination of role change. Role changes for additional access require management approval. Impartner uses the model of least privilege to ensure access is granted only to individuals who need such access in order to perform their job, and such access credentials are reviewed quarterly. All Impartner employees are required to complete security and privacy awareness training as part of onboarding and at least once per year thereafter. All employees are

additionally required to agree to agree in writing to abide by Impartner's privacy and confidentiality requirements.

3. AVAILABILITY AND RESILIENCE OF SYSTEMS AND SERVICES
Systems and services availability and reliability are ensured by taking the following measures:
3.1 Separation. All critical IT and network components are segmented or unconnected to ensure effective periodic testing. Development and Production systems are separate.

3.2 Regular Testing. Impartner systems and services are tested regularly. Additionally, all systems (including power) have backup and redundancy framework to ensure Impartner is able to meet its up-time commitment.

4. AVAILABILITY AND ACCESS IN THE EVENT OF AN INCIDENT
In the event of a physical or technical incident, the availability of and access to personal data are restored by taking the following measures:
4.1 Off Premise Storage. Personal data is stored in Azure on redundant database servers in separate availability zones.

4.2 Backups and Testing. Database backups are taken nightly with quarterly restoration testing.

4.3 RIM. Impartner employs Rigorous Incident Management process for security events that may affect the confidentiality, integrity, or availability of systems or data. If an incident occurs, the security team logs and prioritizes the incident according to its severity level. Events that directly impact customers are assigned the highest priority. This process specifies courses of action, procedures for notification, escalation, mitigation, and documentation.

4.4 Continuous Impartner Security Team Support. To help ensure the swift resolution of security incidents, Impartner’s security team is available 24/7 to all employees. If an incident involves customer data, Impartner will inform the customer and support investigative efforts via Impartner’s security and/or privacy teams.

4.5 Prompt Notification. Impartner's Incident Response Plan includes promptly notifying affected customers of privacy and security incidents in accordance with applicable law and in accordance with applicable agreements between Impartner and its customers. Additionally, affected

customers are notified in the event of any actual or reasonably suspected unauthorized access, use, modification, or disclosure of Customer Data by Impartner or its sub-processors. In such event, Impartner will coordinate communications between its information security and/or data privacy team, as applicable, and the points of contact Impartner has on record for customer. Any breach notifications will contain, at a minimum, a high-level overview of the data subjects impacted, when they were impacted, and the then-current mitigation status.

5. Control Procedures to Ensure the Safety of Processing

Impartner takes a risk-based approach for the regular review, assessment and evaluation of the effectiveness of technical and organisational measures to ensure security of processing. This ensures the protection of relevant information, applications, operating environments (e.g., by network monitoring against harmful effects) and the technical implementation of protection concepts (e.g., by means of vulnerability analyses). By systematically detecting and eliminating weak points, the protective measures are continuously questioned and improved. Additionally, Impartner is aligned with ISO 27001 and performs an annual SOC 2 audit.

6. Monitoring of the Subservice Organisation

Impartner management performs an annual review of its vendors' systems and organisational controls through reviewing audit reports and standardized security questionnaires. Impartner's review includes ensuring that the requisite security controls are in place, and analyzing findings for impact on Impartner and Impartner's platform users.

7. Application and Development Maintenance

Impartner has a defined System Development Life Cycle (SDLC) methodology that governs application development and change management process. SDLC policies and procedures are reviewed annually and updated as needed to reflect changes in the operating environment. Change management is enforced through both policy and technical controls that require Continuous Improvement / Continuous Development (CICD) and separation of responsibility.

8. Personnel Measures

Personnel who have access to personal data receive continuous education and training to ensure (a) data is processed in conformity with the technical

and security measures described herein and (b) that personal data is strictly processed according to the instructions of the data exporter set forth in the applicable agreement and DPA.