ANNEX II - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF DATA RELATED TO THE TRACK BY BETTERCLOUD FEATURES

Access Control:

- AWS: The Track by BetterCloud features are hosted in AWS. Contractual relationships are maintained with vendors in order to provide the features in accordance with our Data Processing Addendum.
- Physical and environmental security: The Track by BetterCloud features are hosted in a multi-tenant, outsourced infrastructure provider. Security controls are audited for SOC 2 Type II and ISO 27001 compliance.
- Authentication: A uniform password policy is implemented for the Track by BetterCloud features. Customers who interact with the products via the user interface must authenticate before accessing non- public customer data.
- Authorization: Customer data related to Track by BetterCloud features is accessible to Customers via application user interfaces and application programming interfaces.
- Industry standard access controls and detection capabilities are implemented for the internal networks that support the Track by BetterCloud features.
- Access controls: Network access control mechanisms, including Virtual Private Cloud (VPC) implementations, security group assignment, and traditional firewall rules, are designed to prevent network traffic using unauthorized protocols from reaching the product infrastructure.
- Intrusion detection and prevention: A Web Application Firewall (WAF) solution is implemented to protect internet-accessible applications. The WAF is designed to identify and prevent attacks against publicly available network services.
- Static code analysis: Security reviews of code are performed, checking for best practices and identifiable software flaws.
- Penetration testing: Annual penetration tests are performed by a reputable third party.
- Product access: A subset of employees may have access to customer data and such access is identified by a unique user ID.

Transmission Control

- In-transit: HTTPS encryption (also referred to as SSL or TLS) is used on the web application and APIs. The HTTPS implementation uses industry standard algorithms and certificates.
- At-rest: Data is encrypted at rest using industry standard practices for security.

Input Control

- Detection: Information about the system behavior, traffic received, system authentication, and other application requests are logged. Alerts are generated for malicious, unintended, and anomalous activities. These alerts are reviewed by the Security team.
- Response and tracking: Records of known security incidents are maintained, including description, dates and times of relevant activities, and incident disposition. Suspected and confirmed security incidents are investigated by the Security team and appropriate resolution steps are identified and documented.
- Communication: Notifications and communications regarding a known data breach will be provided in accordance with applicable laws and the contracts between us and you.

Availability Control

- Infrastructure availability: AWS maintains a minimum of N+1 redundancy to power, network, and HVAC services.
- Redundancy: Backup and replication strategies are designed to ensure redundancy and fail-over protections during a significant processing failure. Customer data is backed up to multiple durable data stores.
- Backups: All databases are backed up and maintained using industry standard methods.