Annex 2
Technical and Organizational Security Measures

The following technical measures are in place to protect the personal data handled by Lookout, Inc.:

- **Encryption of personal data.**
  - Data at rest encrypted using AES-256 algorithm.
  - Employee laptops are encrypted using full disk AES-256 encryption.
  - HTTPS encryption on every web interface, using industry standard algorithms and certificates.
  - Secure transmission of all traffic, internal and external, using by default TLS 1.2.
  - Access to operational environments requires use of secure protocols such as HTTPS.
  - Data that resides in Amazon Web Services (AWS) encrypted at rest as stated in AWS' documentation and whitepapers. In particular, AWS instances and volumes are encrypted using AES-256. Encryption keys via AWS Key Management Service (KMS) are IAM role protected, and protected by AWS-provided HSM certified under FIPS 140-2.

- **Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.**
  - Processing nodes and datastores are replicated across geographically separate locations using cloud provider functionality (Availability Zones) to protect against local outage conditions.
  - Databases are backed up daily with backups maintained for at least one year to provide recoverability from data corruption events.
  - Backups and Availability Zone failovers are tested regularly.

  All infrastructure and applications are built and deployed 'as code', with the ability to recreate an environment from sources in a different region.

- **Processes for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures to ensure the security of the processing.**
  - User activity including logins, configuration changes, deletions and updates are written automatically to audit logs which are forwarded to a central logging system.
  - All actions in the cloud provider system are logged to a central logging system (including cloud API calls, network flow logs).
  - Changes to configuration of security controls (firewalls, VPNs) are logged to a central logging system.
  - Logs are available only to authorized employees, stored off-system, and available for security investigations. Access controls are in place to prevent unauthorized access. Write access to logging data is strictly prohibited. Logging facilities and log information are protected against tampering and unauthorized access through use of access controls and security measures.
  - Logs are maintained for at least one year to facilitate investigations if necessary.
  - A Security Information and Event Monitoring system (SIEM) operates on this logging information to detect anomalies or other indications of security problems. The SIEM generates alerts for such conditions for investigation and action by designated security personnel.
  - Regular vulnerability scans and configuration scans of all components are run at least monthly, with any findings addressed within identified timeframes based on severity.
  - Static and Dynamic Analysis tools are used to maintain security during the development of software.
  - Annual penetration testing for all components, including web and mobile applications.
  - In place a public Vulnerability Disclosure Program and a private Bug Bounty program.
  - All controls are assessed annually be external auditors to meet industry standard certifications.

- **Measures for user identification and authorization.**
  - Access to operational and production environments is protected by use of unique user accounts, strong passwords, use of Multi-Factor Authentication (MFA), role-based access, and least privilege principle.
  - Authorization requests and provisioning are logged, tracked and audited.
  - Customer-generated OAuth tokens are stored in an encrypted state.
  - Keys required for decryption are stored in a secure, managed repository (such as AWS KMS) that employs industry-leading hardware security modules that meet or exceed applicable regulatory and compliance obligations.
  - Access keys used by production applications (e.g. AWS Access Keys) are accessible only to authorized personnel. They are rotated (changed) as required (e.g., pursuant to a security advisory or personnel departure).
  - User activity in operational environments including access, modification or deletion of data is logged.

- **Measures for the protection of Data during transmission.**
  - Remote access to the network via VPN tunnel and end-to-end encryption HTTPS encryption for data in transit (using TLS 1.2 or greater).

- **Measures for the protection of Data during storage.**
  - Customer data is logically separated and attempts to access data outside allowed domain boundaries are prevented and logged. Measures are in place to ensure executable uploads, code, or unauthorized actors are not permitted to access unauthorized data - including one customer accessing files of another customer.
  - Endpoint security software: all production instances have endpoint security software which is monitored for unusual or problematic activity.
  - System inputs recorded via log files.
  - Access Control Lists (ACL).
  - Multi-factor Authentication (MFA).

- **Measures for ensuring physical security of locations at which personal data are processed**
  - Data center controls are maintained by cloud service providers, who are regularly audited for compliance to industry standards (ISO27001, SOC2, PCI, etc.) Corporate facilities (which do not house customer data/personal data) also have the following safeguards:
  - Physical access to all restricted facilities is documented and managed.
  - All information resource facilities (e.g. network closets and storerooms) are physically protected in proportion to the criticality or importance of their function.
  - Access to information resource facilities is granted only to company personnel and contractors whose job responsibilities require access to those facilities.
  - The process for granting card and/or key access to information resource facilities includes the approval of the person responsible for physical facility management.
  - Everyone granted access rights to an information resource facility must sign the appropriate access and non-disclosure agreements.
  - Access cards and/or keys must not be shared or loaned to others.
  - Access cards and/or keys that are no longer required are returned to the person responsible for physical facility management. Cards must not be reallocated to another individual, bypassing the return process.
  - Lost or stolen access cards and/or keys must be reported to the person responsible for physical facility management as soon as practical.

- Cards and/or keys must not have identified information coded into them.
- All information resource facilities that allow access to visitors will track visitor access with a sign-in log.
- Card access records and visitor logs for information resource facilities are kept for routine review based upon the criticality of the information resources being protected.
- The person responsible for information resource physical facility management removes the card and/or key access rights of individuals that change roles within the organization or are separated from their relationship with the organization.
- Visitors in card access-controlled areas of information resource facilities must always be accompanied by authorized personnel.
- The person responsible for physical facility management reviews access records and visitor logs for the facility on a periodic basis and investigate any unusual access.
- The person responsible for physical facility management reviews card and/or key access rights for the facility on a periodic basis and remove access for individuals that no longer require access.
- Signage for restricted access rooms and locations is practiced, yet minimally discernible evidence of the importance of the location is displayed.
- Only individuals authorized by asset owners are permitted to move assets off-site. Details of the individual's identity and role is documented and returned with the asset.
- Equipment is protected to reduce the risks from environmental threats, hazards, and opportunities for unauthorized access.

- **Measures for ensuring events logging.**
  - Remote logging.
  - A central Security Information and Event Management (SIEM) system and other product tools monitor security or activities.

- **Measures for ensuring system configuration, including default configuration.**
  - Lookout has in place a Change Management Policy.
  - Lookout monitors changes to in-scope systems to ensure that changes follow the process and to mitigate the risk of un-detected changes to production. Changes are tracked in our change platform.
  - Access Control Policy and Procedures.
  - Mobile device management.

- **Measures for internal IT and IT security governance and management.**
  - Lookout has established an Information Security Management System (ISMS) in accordance with the ISO 27001:2013 standard. Lookout's Mobile Endpoint Security Platform has been assessed by the US Government Joint Authorization Board (JAB) and authorized as a FedRAMP Moderate system.
  - Information-related business operations continue to be carried out in line with the ISO27001:2013 standard.
  - Lookout has in place a written information security policy, including supporting documentation.
  - The authority and responsibility for managing Lookout's information security program has been delegated a lead of its Information Security (InfoSec) team, who is authorized by senior management to take actions necessary to establish, implement, and manage Lookout's information security program.

- **Measures for certification/assurance of processes and products.**

  - Lookout has been audited by a third party and has achieved SOC2 Type 1 compliance, attesting to its commitment to controls that safeguard the confidentiality and privacy of information stored and processed in its services.
  - Lookout is ISO 27001 and 27017 compliant.

- **Measures for ensuring data minimization.**
  - Detailed privacy assessments are performed related to implementation of new products/services and processing of personal data by third parties.
  - Data collection is limited to the purposes of processing (or the data that the customer chooses to provide).
  - Security measures are in place to provide only the minimum amount of access necessary to perform required functions.
  - Data retention time limits restricted.
  - All deleted customer data follows a similar retention schedule of a recoverable delete between 0-90 days and a permanent delete within 91- 180 days.
  - Restrict access to personal data to the parties involved in the processing in accordance with the “need to know” principle and according to the function behind the creation of differentiated access profiles.

- **Measures for ensuring Data quality.**
  - Lookout has a process that allows individuals to exercise their privacy rights (including a right to amend and update information), as described in Lookout's Privacy Policy.
  - Applications are designed to reduce/prevent duplication. Many application-level checks are in place to ensure data integrity.
  - QA team ensure these items are working as designed and implemented before reaching the production environment.

- **Measures for ensuring limited data retention.**
  - After termination of all subscriptions associated with an environment, customer data submitted to the Services is retained in inactive status within the Services for 90 days, after which it is securely overwritten or deleted from production within 90 days (up to a max of 180 days) and from backups within 180 days.
  - All deleted customer data follows a similar retention schedule of a recoverable delete between 0-90 days and a permanent delete within 91- 180 days.

- **Measures for ensuring accountability.**
  - Customer Privacy Assessments are required when introducing any new product/service that involves processing of personal data.
  - Data protection impact assessments are part of any new processing initiative.

- **Measures for allowing Data portability and ensuring erasure.**
  - Lookout has a process that allows individuals to exercise their privacy rights (e.g. right of erasure or right to data portability), as described in Lookout's Privacy Notices.