ANNEX

Organizational and Technical Measures

The Processor has implemented the measures as described in this exhibit insofar as the respective measure contributes or can contribute directly or indirectly to the protection of the Personal Data under the DPA entered between the Parties.

These measures are commercially reasonable, are aligned with industry standard technical and organizational measures, to protect Personal Data. These measures are consistent with applicable laws and meet the standard of protection appropriate to the risk of processing Personal Data while providing the Processor's services. The Processor will regularly carry out, test, review and update all such measures.

These measures will be subject to technical progress and future developments of Processor's services. As such, the Processor will be permitted to implement alternative adequate measures. In such event, the security level may not be lower than the measures memorialized here. Material changes are to be coordinated with the Controller and documented.

Measures for ensuring physical security of locations at which Personal Data are processed

The Processor has implemented the following entry control measures insofar as Personal Data are processed in the Processor's premises or access to such data from these premises cannot be precluded:

- Unauthorized persons are to be denied entry to the data processing facilities in which Personal Data are processed or used.

- Entry authorizations to office buildings, computer centers, and server rooms are restricted to the necessary minimum.

- Use of effective entry authorization controls through an adequate locking system (e.g., security key with documented key management, electronic locking systems with documented authorizations management).

- Documented and comprehensible processes for obtaining, changing, and rescinding entry authorizations, including routine and documented review whether the granted entry authorizations are up to date.

- Reasonable prophylactic and detection measures regarding unauthorized entry and entry attempts (e.g., routine checks of burglary security system for doors, gates, and windows, burglar alarm, video monitoring, guard service, security patrol).

- Written rules for employees and visitors for dealing with technical entry security measures.

Measure for user identification, authorization and for ensuring events logging

Potential use of data processing systems by unauthorized persons is to be prevented. The Processor has implemented the following access control measures for systems and networks, in which Personal Data are processed or through which access to Personal Data is possible, insofar as the Processor is responsible for the Personal Data access authorizations:

- Persons authorized to use a data processing system will be able to access only the data underlying their access authorization and that Personal Data will be incapable of being read, copied, changed, or removed without authorization during the processing and use of the data and after the data have been stored.

- Access authorizations to Personal Data is restricted to the necessary minimum.

- Access authorizations to Demand Partners systems and non-public networks are restricted to the necessary minimum.

- Use of effective access authorization controls through personalized and unambiguous user identification and a secure authentication process.

- Recording of access, even by administrators.

- For password authentications:

    - Specifications are to be made that ensure continuous password quality of at least twelve (12) characters, four (4) degrees of complexity (upper case, lower case, numbers, special characters), and a change cycle of a maximum of ninety (90) days.

    - Technical test procedures are to be used to ensure password quality.

- If asymmetric key procedures (e.g., certificates, private-public-key-method) are used for authentication, it is to be assured that secret (private) keys are at all times protected by a password (passphrase).

- Implementation of documented and comprehensible processes for obtaining, changing, and rescinding access authorizations, including routine and documented review whether the granted access authorizations are up to date.

- Implementation of reasonable measures for securing network infrastructure (e.g. intrusion detection systems, use of 2-factor authentication for remote access, separation of networks, encrypted network protocols, and so forth).

- Written rules for employees for dealing with the security measures above and the secure use of passwords.

- Use of input controls - there is a possibility to subsequently review and determine whether and by whom Personal Data was entered, altered in, or removed from data processing systems. The Processor has implemented the following input control measures on its

systems, which are used for processing the Personal Data or which enable or convey access to such systems:

- Creation and audit-proof storage of processing protocols.
- Securing log files against manipulation.
- Recording and evaluating unauthorized and failed login attempts.
- Ensuring that no group accounts (including administrators or root) are used.

Measures for ensuring system configuration, including default configuration and encryption of Personal Data

- Ensuring that critical or material security updates/patches will be installed according to the Processor's internal Patch Management Policy: a. in client operating systems; b. in server operating systems reachable via public networks (e.g., webservers); c. in application programs (incl. browser, plugins, PDF-reader, etc.); d. in security infrastructure (virus scanner, firewalls, IDS-systems, content filters, routers, and so forth.); and e. in server operating systems of internal servers.

- Reasonable measures are used for the protection of end-devices, servers, and other infrastructure elements against unauthorized access (such as multi-level virus protection concept, content filters, application firewall, intrusion detection systems, desktop firewalls, system hardening, content encryption).

- The Processor has implemented the following sharing control measures insofar as Personal Data will be received, transferred, or transported by the Processor:
  - Reasonable measures for securing network infrastructure (e.g., intrusion detection systems, use of 2-factor authentication for remote access, separation of networks, encrypted network protocols, and so forth.)
  - Encryption – Processor implements encryption technology which commensurate with the state-of-the-art to be prescribed so that Personal Data will be incapable of being read, copied, changed, or removed during electronic transmission or during transport for storage on data carriers, such as RSA 2048.
    - Data carrier encryption with – state of the art – algorithms and protocols to be classified as secure (e.g., TLSbased protocols) for the protection of mobile devices (notebooks, tablet PCs, smartphones, etc.) and data carriers (external hard drives, USB sticks, memory cards, and so forth).

- Implementation of technical security measures for export and import interfaces (hardware and application related).

Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services and the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident

Personal Data will be protected against accidental destruction or loss. The Processor has implemented the following availability control measures insofar as the processing is required for maintaining productive services:

- Operation and routine maintenance of fire alarms in server rooms, computer centers, and material infrastructure rooms.
- Creating sufficient backups
- Ensuring backup storage in a separate fire compartment.
- Routine backup integrity reviews.
- Systems and data restoration processes and documentation.

An incident would receive immediate attention from all relevant personnel. Once identified and validated, incidents will be reported according to the Processor's security and privacy policies.

Processor's development processes follow secure software development industry-standard practices, which include formal design reviews, threat modeling, and completion of a risk assessment.

Processor uses hash function to de-identify the Personal Data prior to any use.

Measures for ensuring data quality and allowing data portability and processes for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the processing

Personal Data collected for different purposes will be capable of being processed separately. The Processor has implemented the following separation measures insofar as such is within its area of responsibility:

- Logical and/or physical separation of test, development, and production systems.
- Separation of Controller's Personal Data from other data sets including, but not limited to, its own, within the processing systems, and at interfaces.
- Ensuring that Personal Data are constantly identifiable on account of suitable labels; if such are processed for different purposes, including information specifying the respective purpose.

Measures for ensuring limited Personal Data retention

Personal Data is to be deleted, if it is processed for purposes as soon as the knowledge thereof is no longer necessary for the fulfillment of the purpose of the saving in accordance with Fyber's data retention policy.

The Processor has implemented the following measures ensuring data deletion insofar as such is within its area of responsibility:

- Ensuring that the Personal Data are capable of being deleted at any time upon request of the Controller.

- Implementation of processes, tools, and documentation for secure deletion in a manner, such that recovery of the data is not possible given today's state of technology (e.g., through overwriting).

- Providing the employees with specifications regarding how and when data are to be deleted.

Measures for internal IT and IT security governance and management and for ensuring accountability

The Processor has in place internal policies containing formal instructions for data processing procedures; Contractors are being carefully vetted regarding data security; The Processor personnel is being trained periodically to maintain awareness regarding data protection and security requirements.