ANNEX

Organizational and technical measures

The Data Processor has implemented the measures as described in this exhibit insofar as the respective measure contributes or is capable of contributing directly or indirectly to the protection of the personal data under the DPA entered into between the Parties.

The technical and organizational security measures shall be subject to technical progress and future developments of Data Processor's Service(s). As such, the Data Processor shall 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 Data Controller and documented.

1. Entry controls

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

The Data Processor has implemented the following entry control measures insofar as Personal Data are processed in the rooms/buildings of the Data Processor or access to such data from these rooms/buildings cannot be precluded:

1. restricting entry authorizations to office buildings, computer centers, and server rooms to the necessary minimum.
2. effective entry authorization controls through an adequate locking system (e.g., security key with documented key management, electronic locking systems with documented authorizations management).
3. documented and comprehensible processes for obtaining, changing, and rescinding entry authorizations.
4. routine and documented review whether the granted entry authorizations are up-to-date.
5. 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)
6. written rules for employees and visitors for dealing with technical entry security measures.

2. Access controls

Potential use of data processing systems by unauthorized persons is to be prevented.

The Data Processor has implemented the following access control measures for systems and networks, in which contract data are processed or through which access to contract data is possible:

1. restricting access authorizations to DP systems and non-public networks to the necessary minimum.
2. effective access authorization controls through personalized and unambiguous user identification and a secure authentication process.
3. for password authentications:

a. 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.

b. technical test procedures are to be used to ensure password quality.

4. in the event that 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). The requirements contemplated under Sect. 3b above are to be complied with.

5. documented and comprehensible processes for obtaining, changing, and rescinding access authorizations.

6. routine and documented review whether the granted access authorizations are up-to-date.

7. 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.)

8. written rules for employees[1] for dealing with the security measures above and the secure use of passwords[2].

9. ensuring that critical or material security updates/patches shall be installed according to Processor's 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.

3. Access controls

Persons authorized to use a data processing system shall be able to access only the data underlying their access authorization and that personal data shall 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.

The Data Processor has implemented the following access control measures insofar as he is responsible for Personal Data access authorizations:

1. restricting access authorizations to contract data to the necessary minimum

2. effective access authorization controls through an adequate rights and roles concept.

3. documented and comprehensible processes for obtaining, changing, and rescinding access authorizations.

4. routine and documented review whether the granted access authorizations are up-to-date.

5. reasonable measures 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).

6. data carrier encryption with—state of the art—algorithms to be classified as secure for the protection of mobile devices (notebooks, tablet PCs, smartphones, etc.) and data carriers (external hard drives, USB sticks, memory cards, and so forth).

7. recording of access, even by administrators.

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

The Data Processor shall have the following cooperation duties for access controls insofar as it does not manage the access authorizations to the Personal Data itself:

1. documented and comprehensible processes for obtaining, changing, and rescinding access authorizations in its area of responsibility

2. routine and documented review whether the granted access authorizations are up-to-date to the extent possible.

3. notifying the Controller without undue delay, if existing access authorizations are no longer needed.

4. Sharing controls

The Data Controller shall provide the data to be processed in a transmission procedure to be defined in the agreement/mandate. The results of the processing shall also be transferred back to the Data Controller in a defined transmission procedure. The nature of the transmission and the transmission security measures (transmission controls) are to be determined in a manner that does justice to the requirements; in particular, the use of encryption technology commensurate with the state-of-the-art to be prescribed.

Personal data shall be incapable of being read, copied, changed, or removed during electronic transmission or during transport for storage on data carriers and there is the possibility to review and determine at what points a transmission of personal data by data transfer equipment is prescribed.

The Data Processor has implemented the following sharing control measures insofar as contract data shall be received, transferred, or transported by the Processor:

1. 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.)

2. data carrier encryption with—state of the art—algorithms to be classified as secure for the protection of mobile devices (notebooks, tablet PCs, smartphones, etc.) and data carriers (external hard drives, USB sticks, memory cards, and so forth).

3. using—current state-of-the-art—encrypted transfer protocols classifiable as secure (e.g., TLS-based protocols).

4. written rules for employees for dealing with and security of mobile devices and data carriers.

5. Input controls

There is a possibility to subsequently review and determine whether and by whom Personal Data was entered into, altered in, or removed from data processing systems.

The Data Processor has implemented the following input control measures on its systems, which are used for processing the contract data or which enable or convey access to such systems:

1. creation and audit-proof storage of processing protocols.
2. securing log files against manipulation
3. recording and evaluating unauthorized and failed login attempts
4. ensuring that no group accounts (including administrators or root) are used

6. Contract controls

Personal Data, which is processed under contract, shall be capable of being processed only in accordance with the instructions of the Data Controller.

The Data Processor has implemented the following contract control measures:

Data Processes and documentation for

1. selecting (sub)processors with due consideration for technical aspects contemplated under applicable data protection law
2. ensuring (i) the statutorily prescribed initial audit of (sub)processors and (ii) routine subsequent inspections
3. ensuring that the in-house data protection officers shall be notified in timely manner whenever new personal data processing procedures are being introduced or existing personal data processing procedures are being changed
4. obligating all persons commissioned with the processing of personal data to data secrecy
5. routine review that the data processing programs, with the help of which the personal data is processed, are being used in due and proper manner
6. ensuring that the persons commissioned with data processing are familiar with the relevant data protection law and Controller-specific rules and regulations
7. maintaining the expertise of the in-house data protection officer (if appointed)
8. ensuring that the Controller shall be notified without undue delay in the event that personal or otherwise protected information has been unlawfully disclosed
9. ensuring that contract data shall, upon the instructions of the Controller, be corrected, frozen, and deleted without undue delay

7. Availability controls

Personal Data shall be protected against accidental destruction or loss.

The Data Processor has implemented the following availability control measures insofar as the contract processing is required for maintaining productive services:

1. operation and routine maintenance of fire alarms in server rooms, computer centers, and material infrastructure rooms.
2. creating sufficient backups
3. ensuring backup storage in a separate fire compartment
4. routine backup integrity reviews
5. systems and data restoration processes and documentation

8. Separation controls

Personal Data collected for different purposes shall be capable of being processed separately.

The Data Processor has implemented the following contract data separation measures insofar as such is within its area of responsibility:

1. logical and/or physical separation of test, development, and production systems
2. separation of controller data from other data sets including, but not limited to, its own, within the processing systems, and at interfaces
3. ensuring that contract data are constantly identifiable on account of suitable labels; in the event that such are processed for different purposes, including information specifying the respective purpose.

9. Deletion of data

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. Deletion is the obfuscation of stored Personal Data.

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

1. ensuring that the contract data are capable of being deleted at any time upon request of the Data Controller
2. 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)
3. specifications for employees regarding how and when data are to be deleted.