ANNEX TO THE GENERAL CONDITIONS

Data Processing Conditions

The data processing conditions herein referred to as **"DPC"** are an integral part of the General Conditions of Fuzer SA that are applicable under the contract, herein referred to as the **"Contract",** signed between the Client and Fuzer. They replace all previous provisions pertaining to data protection in the General Conditions. In the DPC, the client shall be herein referred to as the **"Client"** and Fuzer SA with company number 0564.795.762 shall be herein referred to as **"Fuzer"**.

1. **Definitions :**

Any capitalised words and expressions used but not defined in the DPC shall have the following meanings:

"Data Protection Legislation" means all applicable laws and regulations relating to the processing of personal data and privacy including the EU Data Protection Directive 95/46/EC and the European Union's General Data Protection Regulation;

"Data Protection Obligations" means the obligations set out in the DPC and the Data Protection Legislation.

"Data Subject" has the meaning set out in the Data Protection Legislation and shall refer, in the DPC to the identified or identifiable individuals listed in **Exhibit 1.1** whose Personal Data are under control of the Data Controller and are the subject of the Processing by the Data Processor in the context of the Services;

"Personal Data" has the meaning set out in the Data Protection Legislation and shall refer, in the DPC to any information relating to the Data Subject that is subject to the Processing in the context of the Services, as listed in **Exhibit 1.2**.

"Processing" has the meaning given to that term in the Data Protection Legislation and "process" and "processed" shall have a corresponding meaning;

"Purposes" shall mean the limited, specific and legitimate purposes of the Processing, as described in **Exhibit 1.3**;

"Regulators" means those government departments and regulatory, statutory and other bodies, entities and committees which, whether under statute, rule, regulation, code of practice or otherwise, are entitled to regulate, investigate or influence the privacy matters dealt with in agreements and/or by the parties to the agreements (as the case may be);

"Sub-Processor" shall mean the subcontractors listed in **Exhibit 1.4**, engaged by the Data Processor to Process Personal Data on behalf of the Data Controller and in accordance with its instructions, the terms of the DPC and the terms of the written subcontract to be entered into with the Sub-Processor; and

"Third Country" means a country outside the European Economic Area that is not considered by the European Commission as offering an adequate level of protection in accordance with Article 25 of the Directive 95/46/EC.

2. **Qualification of Parties**

As part of the provision of the Services, Client engages Fuzer to collect, process and/or use Personal Data on its behalf and/or Fuzer may be able to access Personal Data. The Parties agree that Client is the Data Controller and Fuzer is the Data Processor.

3. **Data Protection**

3.1 The Data Processor and the Data Controller shall comply with the Data Protection Legislation in relation to Personal Data processed under the Contract. The Data Controller shall obtain all required Data Subject consents and ensure all applicable information duties towards Subscribers and Data Subjects are fulfilled.

3.2 Without limiting paragraph 3.1, the Data Processor warrants, represents and undertakes to the Data Controller that:

(A) it shall only Process the Personal Data:

(1) on behalf of the Data Controller and in accordance with the DPC, for the Purposes and the documented instructions of the Data Controller, or if reasonably necessary to provide the Services in accordance with the Contract; or

(2) as required by applicable mandatory laws and always in compliance with Data Protection Legislation;

(B) it shall not otherwise modify, amend and/or alter the Personal Data or use it for its own purposes, always subject to Article 3.2 (A) (2);

(C) it shall not transfer or disclose any Personal Data to any third party without the prior written consent of the Data Controller, except that the Data Processor shall be entitled to engage any third party (including any other data processor, such as cloud computing service providers, (sub)contractors or other sub-processors) for the Processing of Personal Data to the extent necessary to fulfill its contractual obligations under the Contract. In addition:

(1) prior to any such transfer, disclosure or engagement the Data Processor shall enter into a written agreement with each such approved third party containing obligations on it in relation to Personal Data; and

(2) the Data Processor shall remain responsible to the Data Controller for any breach of the Data Protection Obligations by any third party sub-contractor or sub-processor it appoints or to whom it discloses or transfers Personal Data.

(D) it shall Process the Personal Data solely in the European Economic Area and/or in a third country with an adequate level of Protection (in accordance with Article 25 of the Directive 95/46/EC) and, thus, shall not (fully or partially) process the Personal Data in any Third Country without the prior written consent of the Data Controller, except if appropriate safeguards in conformity with the GDPR are in place (such as e.g. the signing of the standard contractual clauses of the European Commission for the transfer of personal data to processors established in third countries (2010/87/EU) or approved binding corporate rules or adherence to an approved

code of conduct). With the exception of the latter circumstances:

(1) where the Data Processor processes Personal Data of the Data Controller in a Third Country, the Parties commit to enter into a data transfer agreement for those processing activities in the Third Country in a form based on the standard contractual clauses launched by virtue of the EU Commission Decision 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC (the "Model Contract Clauses"); and

(2) where the Sub-Processor processes Personal Data in a Third Country ("Third Country Sub-Processor"), the Data Processor commits to enter into a data transfer agreement with the Sub-Processor that is based on (and incorporates) the Model Contract Clauses.

(E) it shall maintain data secrecy in accordance with applicable Data Protection Legislation and shall take all reasonable steps to ensure that:

(1) only those Data Processor workers that need to have access to Personal Data are given access and only to the extent necessary to provide the Services; and

(2) the Data Processor workers entrusted with the processing of, or who may have access to, Personal Data are reliable, familiar with the requirements of data protection and subject to appropriate obligations of confidentiality and data secrecy in accordance with applicable Data Protection Legislation and at all times act in compliance with the Data Protection Obligations;

(F) it has implemented (and shall comply with) all appropriate technical and organisational measures (as specified in **Exhibit 1.5**) to ensure the security of the Personal Data, to ensure that processing of the Personal Data is performed in compliance with the applicable Data Protection Legislation and to ensure the protection of the Personal Data against accidental or unauthorised access, alteration, destruction, damage, corruption or loss as well as against any other unauthorised or unlawful processing or disclosure ("Data Breach"). Such measures shall ensure best practice security, be compliant with Data Protection Legislation at all times and comply with the Data Controller's applicable IT security policies;

(G) the Data Processor shall provide the Data Controller with such assistance and co-operation as the Data Controller may reasonably request to enable the Data Controller to comply with any obligations imposed on it by Data Protection Legislation in relation to Personal Data processed by the Data Processor, including but not limited to:

(1) on request of the Data Controller, providing written information regarding the technical and organisational measures which the Data Processor has implemented to safeguard Personal Data;

(2) disclosing relevant details in respect of any and all government, law enforcement or other access protocols or controls which it has implemented;

(3) notifying the Data Controller as soon as possible and as far as it is legally permitted to do so, of any access request for disclosure of data which

concerns Personal Data (or any part thereof) by any Regulator, or by a court or other authority of competent jurisdiction. For the avoidance of doubt and as far as it is legally permitted to do so, the Data Processor shall not disclose or release any Personal Data in response to such request served on the Data Processor without first consulting with and obtaining the written consent of the Data Controller;

(4) notifying the Data Controller as soon as possible of any legal or factual circumstances preventing the Data Processor from executing any of the instructions of the Data Controller; and

(5) notifying the Data Controller as soon as possible of any request received directly from a Data Subject regarding the Processing of Personal Data, without responding to such request (unless authorized in writing by the Data Controller to do so).

3.3 The Data Processor shall inform the Data Controller immediately of any inquiry, complaint, notice or other communication in connection with the Services or the Data Controller's compliance with Data Protection Legislation from any Regulator or any individual, which the Data Processor or any third party appointed by the Data Processor receives. The Data Processor shall provide all reasonable assistance to the Data Controller to enable the Data Controller to respond to such enquiries, complaints, notices or other communications and to comply with Data Protection Legislation. For the avoidance of doubt, the Data Processor shall not respond to any such inquiry, complaint, notice or other communication without the prior written consent of the Data Controller.

3.4 The Data Processor shall notify the Data Controller immediately in writing if it becomes aware of any Data Breach and provide the Data Controller, as soon as possible, with complete information relating to a Data Breach, including, without limitation, the nature of the Data Breach and the Personal Data affected, the categories and number of Data Subjects concerned, the number of personal data records concerned, measures taken to address the Data Breach, the possible consequences and adverse effect of the Data Breach and any other information the Data Controller is required to report to the relevant Regulator or Data Subject. The Data Processor shall maintain a log of Data Breaches including facts, effects and remedial action taken. The Data Processor shall, at its own cost, take all reasonable steps to restore, re-constitute and/or reconstruct any Personal Data which is lost, damaged, destroyed, altered or corrupted as a result of a Data Breach, within a reasonable timeframe and as if they were the Data Processor's own data, and shall provide The Data Controller with all reasonable assistance in respect of any such Data Breach. The Data Processor shall also provide all reasonable assistance to the Data Controller in relation to the Data Controller's compliance with the Data Protection Legislation.

3.5 Where the Data Controller is legally required to provide information regarding the Personal Data and its processing to any Data Subject or third party, the Data Processor shall provide reasonable support to the Data Controller in the provision of such information.

3.6 The Data Processor shall implement appropriate technical and organisational measures to provide the Data Controller with co-operation and assistance in complying with any Data Subject rights under the Data Protection Legislation (including access requests, right to be forgotten and data portability) received by, or on behalf of, or in connection with the Data Controller or in the Contract.

3.7 The Data Processor shall support and assist the Data Controller in fulfilling its legal requirements with regards the creating and updating of a process register and undertaking required risk assessments for the Processed Personal Data, especially but not limited to changes in the technical and organizational measures. The Data Processor shall maintain written records of all categories of processing activities carried out on behalf of the Data Controller containing such information as required under Data Protection Legislation and any other information the Data Controller reasonably requires and shall make such records available to the Data Controller on request in a timely manner, where reasonably required by the Data Controller to demonstrate compliance by the Data Controller with its obligations under Data Protection Legislation, which the Data Controller may disclose to any relevant Regulator.

3.8 Data Processor shall allow for and shall contribute to reasonable demands for audits conducted by an independent auditor mandated by Data Controller to conduct, at the Data Controller's cost, data privacy and security audits, assessments and inspections concerning the Data Processor's data security and privacy procedures relating to the processing of Personal Data, and its compliance with the Data Protection Obligations. Data Processor and Data Controller agree to limit the audits to a strict minimum and with a maximum of once every calendar year, unless serious reasons for an earlier audit would exist or if a data protection authority would require so. Certifications and existing audit reports will be used to avoid audits.

3.9 Upon the termination of the Contract, the Data Processor shall without undue delay cease all use of Personal Data and shall delete or anonymize all Personal Data and copies thereof in its possession, unless the law requires further storage of such Personal Data.

4. **Liability**

As per the General Conditions.

5. **Term**

The DPC shall be valid as from the 25th of May 2018 and shall survive the expiration or termination of the Contract for such period as the Data Processor still has access to Personal Data subject to the Contract.

6. **Entire agreement**

The DPC shall supersede any other written or oral negotiations, agreements, understanding or representations between the Parties with respect to privacy and the protection of the Personal Data Processed under the Contract.

7. **Modifications**

The DPC may be supplemented, amended or modified by Fuzer only if such supplement, amendment or modification is implied to fulfill the Data Protection Legislation.

8. **Governing law – jurisdiction**

The governing law and jurisdiction as agreed upon in the Contract.

Exhibit 1

1.1 Data Subjects

The Personal Data subject to Processing under the DPC belong to the following categories of Data Subjects:

- *End-users working for the Data Controller and which are provided by the Data Controller with Services supplied by the Data Processor. They are mainly employees and/or representatives of the Data Controllers but not exclusively.*

1.2 Personal Data

The categories of Personal Data subject to Processing under the Contract might be the following:

- *Identifying data (i.e. data which can directly identify the person), if the Data Processor receives these data from the Data Controller as they are necessary to perform services such as legal inquiry*
    - Contact details (i.e. e-mail, phone, addresses)
    - Generic details (i.e. name, data of birth, ID-card number, gender, Belgian ID (y/n), place of birth)
    - ID card copy (i.e. physical and scanned copy of ID-card)
    - National registration number (i.e. RRN)
    - Nationality

- *Contract data (i.e. data related to contract fulfilment)*
    - Authentication details (i.e. username, password)
    - Technical & account information for the use of the products and services (i.e. DB/DC model, mailbox alias, account ID, subscriber ID)

- *Traffic, location and usage data (i.e. data derived from the use of products/services)*
    - Geo-location (i.e. cell ID, triangulation coordinates)
    - Traffic information (metadata) (i.e. imsi, imei, ip address, mac address, a number, b number, URL, call detail records for telephony and internet)

- *Content data (i.e. content created by the user when using products/services) , to the extent permitted by law (such as the legal provisions pertaining to telecommunication secrecy)*
    - SMS/MMS services (i.e. content of SMS/MMS)
    - Telephony services (i.e. content of voice calls)
    - Voicemail recordings (only relevant in Light Client)
    - Data services (i.e. content of mail)

- *The processing of data derived from the use of products / services may exceptionally result in the processing of special categories of personal data, such as personal data concerning a natural person's sex life or sexual orientation, health data, racial or ethnic origin, trade union membership, political opinion or religious or philosophical belief.*

1.3 Purposes

The Data Controller entrusts the Data Processor with the Processing of Personal Data for the following purposes:

1. *Support to Regulatory Requests, including requests of legal authorities (such as legal inquiry and legal interception requests)*
2. *Client Service Delivery (incl. billing)*
3. *Fraud Management*
4. *General Product, Service and Network Management*
5. *Anonymized and aggregated reporting for 3rd parties*
6. *Offering of commercial products or services to third parties containing or based on anonymized and/or aggregated location, traffic, network and/or usage data.*

1.4 Sub-Processors

The Data Controller hereby agrees to the following list of Sub-Processors, might be engaged by the Data Processor for the Processing of Personal Data in under the Contract:

Name	Address	Company Nbr
COLT TECHNOLOGY SERVICES N.V.	Cullinganlaan, 2H, 1831 Diegem, Belgium	BE 0461.455.625
TELENET B.V.B.A.	Liersesteenweg(MeSK) 4, 2800 Mechelen, Belgium	BE 0473.416.418
ESCAUX S.A.	Chaussée de Bruxelles 408, 1300 Wavre, Belgium	BE 0452.498.367
INTERXION BELGIUM S.A.	Wezembeekstraat 2 bus 1, 1930 Zaventem, Belgium	BE 0471.625.579

1.5 Security Measures

Description of the technical and organizational security measures implemented by the Data Processor:

1. The Data Processor is committed to helping the Data Controller protecting the security of the Personal Data. It has and will maintain and apply IT security policies and practices that are mandatory for all its employees and external providers. It reviews these policies regularly and amends them when required. As a consequence, the Data Processor is capable of, and shall, implement, maintain, and regularly verify the continued effectiveness of appropriate technical and organizational measures, as further described in its applicable IT security policies, to ensure a level of security appropriate to the risk associated with the nature of the Personal Data and with the Services being provided, including but not limited to appropriately:

- Assessing and minimizing risks associated with providing the Services using the Personal Data, including the risks of unauthorized collection, access, use, and disclosure and of accidental or unlawful destruction, loss, or alteration;
- Using pseudonymization and encryption;
- Ensuring the ongoing confidentiality, integrity, availability, and resiliency of processing systems and services;
- Testing, assessing, and evaluating the effectiveness of technical and organizational measures for ensuring the security of the Personal Data and the Services.

2. The Data Processor has adopted adequate policies and implemented appropriate procedures to avoid that unauthorized persons will have access to the data systems used to process the Personal Data and that any persons it authorizes to have access to the Personal Data will protect and maintain the confidentiality and security of the Personal Data.

3. The Data Processor has and will maintain appropriate physical entry controls, such as entry badge systems and alarms, to protect against unauthorized entry into its facilities, including its data centers. Where necessary, the Data Processor has implemented and will maintain logging and audit trail mechanisms.

4. The Data Processor shall ensure that all personnel involved in processing the Personal Data are authorized personnel with a need to access the data, are bound by appropriate confidentiality obligations, and have undergone appropriate training in the protection and handling of the Personal Data.

5. The Data Processor shall not copy or reproduce any of the Personal Data except as technically necessary to provide the Services (e.g. for data backup for business continuity or disaster recovery purpose) or to comply with statutory data retention rules, or as agreed upon in the DPC.

6. The Data Processor shall maintain or enable a minimum of physical and/or logical segregation of the Personal Data from any other data of the Data Processor or a third party.

7. The Data Processor warrants that it monitor its infrastructure and has implemented response policies and procedures appropriate to the risks associated with the Personal Data.