ANNEX 1
DATA PROCESSING STATEMENT

Revision history:

Version	Date	Description
1.0.	September 1, 2018	Part 1. Data Processing Statement Part 2. Standard Clauses for Data Processing
1.1.	January 25, 2020	Sub-processor Make Marketing Magic is removed. Overall language is improved to clarify the agreements of this DPA.
2.0	April 10, 2020	1. Part 2 Standard Clauses for Data Processing is integrated into the The NLdigital Terms 2020 deposited by NLdigital at the District Court Midden-Nederland, location Utrecht. 2. This version is the Data Processing Statement. Part 2 of the document (Standard Clauses for Data Processing) is removed. 3. Digibites Technology VoF is removed from the list of Fusix suppliers of Business Personal Data. 4. Changes in clause 5.2: addition of statements on the Network Monitoring data

This Data Processing Statement constitutes practical arrangements on personal and other data processing that were made by and between Fusix Networks B.V. and a customer to whom Fusix provides its service or product.

Together with Section 2 of The NLdigital Terms 2020 'Standard clauses on data processing' this Data Processing Statement forms a data processing agreement ("DPA") as meant in article 28, paragraph 3 of the General Data Protection Regulation (GDPR).

The Statement applies to all Fusix services and products that the company provides to a Client under the Agreement or proposed to provide by submitting a service offer.

Together with other applicable documents references in the Agreement, the DPA contains a complete agreement between Fusix and the Customer with regard to any confidential or sensitive information ("data") including but not limited to Personal Data that is (i) collected or processed by Fusix in its own name or on behalf of the Customer, or (ii) collected or processed by the Customer in its own name or on behalf of its customer(s) using any of the Fusix services or products.

All Fusix Services are provisioned "business-to-business", therefore the Parties to this DPA are (i) Fusix Networks B.V. ("Fusix") and (ii) the legal business entity that has entered into the Agreement with Fusix ("Client").

General information and Definitions

Contact: If Client has any queries about this DPA or Personal Data processing by Fusix, it should contact Fusix on privacy@fusix.nl and/or by phone: +31 (0) 85 401 4441.

Adjustments: Fusix will be entitled to adjust this Data Processing Statement, if it feels that such adjustment is necessary for a continued provision of an appropriate level of security for any of its Services or products. It will record any significant adjustments in a revised version of this Data Processing Statement, and will notify Clients of said adjustments via regular communication channels, if substantial changes are made.

Capitalized terms and abbreviations that are not defined in the DPA shall have the meaning attributed to them in the applicable parts of the Agreement: Service Order, Acceptable Use Policy, Service Description, NLdigital Terms 2020 and any other document, if referenced in the Agreement.

Definitions. The following terms have the meaning attributed in the DPA:

Agreement: the agreement concluded between the Client and Fusix, on whose basis Fusix provisions one or more of its services or products, the DPA being a part of each Agreement.

Dutch Data Protection Authority (AP): the regulatory agency outlined in Section 4.21 of the GDPR.

GDPR: the General Data Protection Regulation 2016/679 in the European Union law on data protection and privacy for all individuals in the European Union (EU) and European Economic Area (EEA).

Data: information, including but not limited to Personal Data that is being collected and/or processed by either Party in its capacity of an ICT supplier. Data that is processed by Fusix is in its capacity of service provider to the Client is specified in Section 5 of the Data Processing Statement.

Client Data means any Data that the Client processes in its own name or on behalf of its customer(s) using any of the Services or products provisioned by Fusix under the Agreement. With regard to the Client Data, the Client may be the Data Controller or the Data Processor who processes the Client Data on behalf of its customer(s), however in the relationship between the Client and Fusix, the Client shall have the capacity of the Data Controller.

Data Controller: a party that determines the purpose and means of Data processing.

Data Processor: a party that, in its capacity of an ICT supplier, processes Data on behalf of its customer(s) as part of performance of its ICT services.

Data Processing Statement: Part 1 of this DPA in which Fusix provides information on the intended use of its Services and products, any security measures which have been implemented, sub-processors, Data breach, certification and dealing with the rights of Data Subjects, among other things.

Data Subject: a natural person who can be identified, directly or indirectly.

Client: a legal entity that entered into an Agreement with Fusix. For the purpose of this DPA, Client uses one or more of the Services mentioned in clause 3 of the Data Processing Statement to collect and/or process Data in its role of a Data Controller and/or a Data Processor for its customer(s).

Personal Data: any and all information regarding a natural person who has been or can be identified, as outlined in Article 4.1 of the GDPR.

Data Processing Agreement: Part 1 and Part 2 of this Data Processing Agreement that together constitute the data processing agreement within the meaning of Article 28.3 of the GDPR.

Confidentiality agreement and duty of confidentiality: an agreement that was made between Fusix and the Client with the purpose to regulate exchange of confidential information. Duty of

confidentiality is obligation of a Party that receives confidential information from the other Party under a Confidentiality agreement.

Party, Parties: Client and Fusix Networks B.V. are individually referred to as a "Party" and collectively as "Parties".

RIR means a Regional Internet Registry. There are 5 RIRs in the world: RIPE NCC, LACNIC, ARIN, APNIC, AfriNIC.

PART 1: DATA PROCESSING STATEMENT

Part 1 describes what information ("Data") – including but not limited to Personal Data in the meaning of the General Data Protection Regulation 2016/679 in the European Union law ("GDPR") – is being collected and/or processed by Fusix, security measures implemented to protect such Data and specific aspects of Personal Data processing as statutory required by GDPR.

Data Processing Statements

1.   Fusix adheres to the Standard clauses on data processing, which can be found in Section 2 of The NLdigital Terms 2020 deposited by NLdigital at the District Court Midden-Nederland, location Utrecht.

2.   This Data Processing Statement applies to all Services and products of any kind and to all offers issued by Fusix.

3.   Functional description of Services

Internet Services are designed to transport IP-packets ("**traffic**") between Internet applications of the Client and the users of these applications on the public Internet

Carrier Services are designed to transport Data a between two or more locations of the Client's network. The Carrier Services are used by Clients who have network nodes in different physical locations and wish to establish connectivity between them with the goal to transport Client Data between these nodes.

Consultancy Services and stand-by network troubleshooting assistance are designed to share with Clients the expertise of Fusix in design, configuration, implementation, management, operation and change/upgrade of IP networks. They are provided to Clients who have or plan to have their own IP network and wish to receive advice or practical assistance with deployment, management or urgent on-request troubleshooting of their network.

Additional information regarding Fusix Services and use examples can be found in the "**Fusix Service Description**" and in "**Fusix Service Level Agreement**". Specific parameters of a Service that Fusix provides to each Client can be found in a relevant **Service Order.**

4.   Intended use of Fusix Services and products with regard to Data processing by Client

4.1.   Fusix Services must be used in accordance with the Acceptable Use Policy that is published on the Fusix web-site www.fusix.nl and with other terms of the Agreement.

4.2.   Fusix has **no** knowledge as to the content of the Client Data that is being transmitted or otherwise processed by the Client using the Fusix Services and therefore does not know which categories of Personal Data (if any) and which Data Subjects (if any) are involved in relation to such Client Data. If any of the Services is used by the Client or its customers to send/receive any sensitive, confidential or Personal Data content, including but not limited to special categories of Personal Data or Data regarding criminal convictions and offences, it will be **the responsibility of the Client** to use appropriate security measures to protect such Data. It is up to the Client to assess security risks and to determine and implement relevant security measures in proportion to the assessments. As always, Fusix encourages all its Clients to use proactive security measures such as for example encryption, VPN, separation of publically and internally accessible Internet applications, anonymization and pseudonymization of Personal Data etc. to protect confidentiality of any Data that they process when using the Fusix Services.

5.   Data processing by Fusix

Fusix processes different types of Data as described in this Section 5 in order to provision and maintain its Services and products, provide technical support and maintain business relationships with existing Clients and potential customers.

5.1.   Business Contact Personal Data

As a part of the process to install, provision and maintain its Services, Fusix requests its Clients to provide contact information of the Client's Representatives (natural persons) for commercial, billing and technical communication. This information constitutes Personal Data as defined by the GDPR ("Business Contact Personal Data").

Fusix is the Controller and Processor of Business Contact Personal Data of the Client's Representatives. The purposes, goals and processing methods that Fusix uses with regard to the Business Contact Personal Data are explained in the **"Fusix Privacy Policy"** publically available on the Fusix website www.fusix.nl for all individuals who may want to or were required to provide their Personal Data to Fusix.

5.2.   Network Monitoring and Network Flow data.

Network Flow data is digital records ("metadata") that describe and characterize connections made over an IP network, including elements such as IP addresses and port numbers for source and destination endpoints, protocols, used bandwidth, timestamps and network interfaces, but excluding the content ("payload") of communication between the endpoints.

Network Flow data contains (among other identifiers) IP addresses of network equipment and servers, usually web-sites or other types of publically available Internet-based applications that are reachable from the public Internet, however it does not provide any direct or indirect reference to natural persons and therefore does not qualify as Personal Data in the meaning of GDPR.

Network Monitoring data is information that describes status and performance parameters of the network equipment and connections that are a part of the Fusix Network Service delivery infrastructure. In case Fusix provides network management and on-request advanced troubleshooting assistance to a Client, the Monitoring data will describe network equipment and connections that are a part of the network infrastructure of the Client.

Network Monitoring data contains (among other identifiers) IP addresses assigned to network equipment and servers, however it does not provide any direct or indirect reference to natural persons and therefore does not be qualified as Personal Data in the meaning of GDPR.

With regard to IP addresses in particular, provisioning of Services by Fusix requires routing of IP-packets between IP addresses of endpoints. The routing is based on knowing, which ISP network announces the destination IP address, so that the IP-packets can be sent there. For the purpose of routing IP-packets, Fusix processed the following information concerning IP addresses:

(i) **Full Internet Routing Table.** Each ISP on the Internet announces its own IP address blocks to its direct peers. Combined, these announcements constitute the Full Internet Routing Table that is used by all ISPs for sending out traffic. The Internet Routing Table is public and for each ISP network on the Internet it provides (i) its AS number, (ii) which IP address blocks it announces via Boarder Gate Router protocol to other networks on the Internet. The Internet Routing Table has no reference whatsoever to natural persons, therefore the use of this information by an ISP should not be qualified as processing of Personal Data in the meaning of GDPR.

(ii) **Allocation of Fusix IP addresses to Clients.** Fusix Clients who do not have their own Internet Resources (IP addresses) are allowed to use the IP addresses of Fusix for the Term of the Agreement. Since Fusix relationship with all Clients is business to business, Fusix provided its IP addresses to the Client's organization, which in its turn re-distributes the IP addresses to servers or to another kind of device that the Client decides to give access to the Internet This re-distribution process is controlled by the Client. Fusix keeps confidential the information about which IP address are used by which Client's organization. This information is kept in an internal system for which Fusix has implemented relevant organizational and technical security measures explained in Section 9.

Network Flow and Network Monitoring data is confidential information, thus with regard to it Fusix and Customer have a duty of confidentiality as stated in the NLdigital 2020 Section 1 General Provisions, Article 5 Confidentiality.

Network Flow and Network Monitoring data is collected and used by Fusix for provisioning, monitoring, maintenance, troubleshooting and billing of such Fusix services as for example Internet and Carrier services, Network Consultancy, and network management and stand-by troubleshooting assistance to Clients.

Network Monitoring and Flow data that Fusix collects with regard to the IP-packet transmissions is:

- Bandwidth
  Bandwidth is measured in Megabits that were transferred per second to/from the IP addresses of a Client.

- Per individual IP-packet transfer request, Fusix collects and processes the following information:
  - IP protocol, such as TCP, UDP, ECMP;
  - number of packets per second;
  - number of bits per second;
  - source and destination IP address;
  - source and destination port;
  - Source and destination MAC address of the routers of the endpoint networks.

6.   Fusix processes all Data within the EU/EEA.

7.   For processing of Business Contact Personal Data, Fusix uses a number of business-support products of 3rd parties, some of which process data outside the EU/EEA as explained below:

- MailChimp ("The Rocket Sience Group LLC d/b/a MailChimp") is used to create a Company News Letter of Fusix and to send it out via e-mail.
  To protect Personal Data that is being processed outside the EU/EEA, MailChimp participates in and has certified its compliance with the EU-U.S. Privacy Shield Framework and the Swiss-U.S. Privacy Shield Framework.

- Kayako Ltd. provides to Fusix a Ticket Management Software as a Service.
  To protect Personal Data that is being processed outside the EU/EEA, Kayako Ltd. and Fusix have concluded a Data Processing Agreement that binds Kayako Ltd. to only transfer Personal Data outside the EU/EEA, where such transfers are regulated by the EU Rules, in compliance with the applicable EU Rules.

- Exact On-Line B.V. provides to Fusix its Accountancy Software as a Service. It processes Data in the EU/EEA.

- MoneyBird provides to Fusix its Invoicing Software as a Service. It processes Data in the EU/EEA.

8.   Retention of Data

8.1.   Except when required otherwise by any applicable legislation, statutory obligations or by a business information management system that is in use by Fusix, if Fusix was processing any Personal Data on behalf of the Client, Fusix will delete such Personal Data within 3 (three) months in such a manner that the Personal Data will no longer be usable and will be rendered inaccessible.

8.2.   Fusix will have the right to archive the Network Flow Data that has been collected during the Term of the Agreement. A duty of confidentiality will apply to Fusix with regard to the archived Data. Fusix will be allowed to use the archived Data only as an evidence of the Fusix Service performance, as needed due to regulatory requirements and/or for research and development purposes related to the Fusix Services.

Security policy

9. **Fusix has implemented security measures to protect confidentiality, integrity, availability and resilience of its Services. These measure include among others:**

- Policies and procedures that govern protection of confidential Data and provide guidance to the Fusix staff on a proper disposal of physical Data and equipment that contains confidential Data;
- Safeguard measures to protect electronic and physical Data;
- "Need to know" standard regarding access to confidential Data;
- Fusix enters into Memoranda of Understanding and/or Non-Disclosure Agreement prior to the disclosure or receipt of confidential information with third parties;
- Routine training on confidentiality for the Fusix staff;
- Access to information sharing systems, such as Fusix Customer Portal, is password-protected and is possible only for authorized user accounts. Authorization of new user accounts is controlled by a Client Representative;
- Network management systems capable to make a change in configuration of the Fusix backbone and/or Clients' connections are accessible only from the Fusix private network and not from the public Internet;
- There is a stand-alone management access to the Fusix backbone devices that ensures availability of access to the backbone for immediate troubleshooting;
- Service provisioning tasks are automated and use templates that allow to enter only valid Service configuration commands;
- 24/7 automated monitoring of performance of the Fusix backbone;
- 24/7 automated monitoring of performance of the Clients' connections;
- 24/7 "wake-up" alert on performance measurements require attention/troubleshooting;
- Regular maintenance work reduce the risk level of unexpected issues on the Fusix Service delivery infrastructure;
- Fusix Service delivery infrastructure is deployed redundantly and single points of failure are avoided when possible;
- Network Flow Data is monitored to detect on-going threats;
- Clients have on-line 24/7 tools to activate preventive filtering of incoming IP traffic;
- Use of Resource Public Key Infrastructure in combination with 'invalid = reject' policy to improve protection of the Client Data against route and IP address hijacks;
- Promotion of Resource Public Key Infrastructure among ISPs;
- Promotion of Route Origin Authorization certificates among legitimate holders of Internet Resources to assist them safeguard their Internet Resources. Each ISP can create a ROA certificate for its network, which is a cryptographically signed object that states which Autonomous System (AS) is authorized to announce specified blocks of IP addresses;
- With regard to Personal Data, Fusix follows the "privacy by default" principle: it asks only a minimum set of Business Contact Personal Data as required for provisioning of its Services, statutory obligations of the company and efficient business to business communication with existing, ex- and potential customers.

Data leak protocol

10.   In the unfortunate event that something does go wrong with regard to processing of Personal Data by Fusix, where the reporting obligation applies to Fusix under the GDPR, Fusix will use a Data leak protocol to ensure that the Client is notified of the incident.

Examples of possible Data security incidents include, but are not limited to:
- Loss or theft of Fusix equipment, such as cell phone, laptop;
- Loss, theft or improper disposal of hard copy documents;
- Misdirection of an e-mail;
- Computer hacking, social engineering;
- Unauthorized disclosure on the public Internet or a social media;
- Unauthorized copying of data to personal electronic devices;
- Improper disposal of Fusix equipment;
- Improper disposal of Client's equipment.

Incidents will be reported electronically to the Client's designated Representative:

Name:
E-mail:

If Client did not provide a designated point of contact for Data security communication, incidents will be reported to a general point of contact as provided in the Client's Agreement.

Each incident report will contain at least the following information:
- incident description and time;
- any additional information usable for risk assessment of the harm, such as likelihood of identification of natural persons, whether the confidential information was actually accessed, how far the information was protected etc.