Statement on the Protection of Personal Data

STATEMENT ON THE PROTECTION OF PERSONAL DATA IN ACCORDANCE WITH THE GENERAL REGULATION ON THE PROTECTION OF PERSONAL DATA (EU 679/2016)
Dominion Hosting Hodling S.p.A. (hereinafter "DHH") as the first contractual partner guarantees

1. Introductory provisions

1.1
By confirming the General Terms and payment of the pro forma invoice for the services provided by the company DHH (hereinafter: Contractual services), the second contractual partner has entered into a contractual relationship.

1.2
This Statement is considered part of the contractual relationship and ensures the regulation of mutual relations in accordance with the General Regulation on the Protection of Personal Data EU 679/2016 (hereinafter: Regulation).

1.3
Contract partner DHH will, in mutual relationship and in accordance with the Regulation, have the status of a processor (hereinafter: Processor).

1.4
The second contractual partner will, in mutual relationship and in accordance with the Regulation, have the status of a data controller (hereinafter: Data Controller).

1.5
The terms used in this Statement have the same meaning as set out in the Regulation.

1.6
The processor will keep a proper record of all received personal data necessary for the performance of the Contractual Services.

1.7
Personal data that the Processor will encounter unintentionally in the performance of the Contractual Services shall also be considered as given. The Processor will keep a proper record of this personal data.

1.8
The processor will also keep a proper track record, including processing purposes (Annex 1).

1.9
The Processor will use the received collection or personal data contained therein exclusively for the performance of the Contractual services.

2. Information security and compliance with the Regulation

2.1
The Processor has accepted and in its operation consistently implements appropriate technical and organizational measures that ensure protection of personal data and the exercise of rights in connection with them in accordance with the Regulation (Articles 28 and 32).

2.2
Minimum technical and organizational measures to prevent the unintentional or deliberate unauthorized alteration, destruction, loss or unauthorized processing of personal data include:

- physical, technical and logical security of premises, hardware and system software, including ICT input/output units;
- technical and logical protection of user software;
- technical and logical prevention of unauthorized access to personal data when transmitted, including transmission by telecommunication means and networks;
- effective ways of blocking, destroying, erasing or anonymizing personal data when the purpose, for which it was collected, is completed;
- provision of audit trails for subsequent identification, time of entry of individual data into the records of personal data, use, interventions, insights or other processing and the
- identification of providers of these activities (keeping records of the processing and transmission of personal data);
- written commitments to confidentiality by persons, who are authorized to process personal data;
- other appropriate measures provided for by the Regulation (Article 32).

2.3
The Processor guarantees that, in the performance of Contractual Services, it shall take into account and comply with all the terms, requirements and standards which, in relation to the security of personal data, are defined by their respective mutual agreements, the Regulation and good practices in information security.

2.4
The Processor also fulfills all the provisions of the Regulation and good information security practices in connection with the design and storage of audit trails.

3. Obtaining, processing, forwarding and retention of personal data

3.1
The Data Controller acknowledges that all personal and related data that are subject to processing or performance of the Contractual Service, is obtained legally and in a manner consistent with the provisions of Articles 6 (1), 7 (1), 8 and 9 (2) of the Regulation.
3.2
The Data Controller confirms that all individuals are informed in a clear, understandable manner in writing, of the principles of collecting, processing, forwarding and retention of personal data as defined in Article 5 of the Regulation.

4. Individual rights

4.1
The Data Controller permits all individuals, in connection with their personal data, to exercise all the rights referred to in Articles 12 to 22 of the Regulation.
4.2
In accordance with the provisions of Articles 37, 38 and 39 of the Regulation, the Processor appointed the Commissioner for the security of personal data and defined his (her) powers, obligations and responsibilities.

5. Data Controller rights

5.1
At any time, the Data Controller may, at his own expense and with the assistance of an independent auditor, verify the performance of Contract Services at the Processor and, in particular, the implementation of appropriate technical and organizational measures, which ensure information security and security of personal data and compliance with the Regulation and good practices in information security.
5.2
Data Controller may limit or prohibit the Processor's co-operation (including transfer of information) in carrying out the Contract Services with individual sub-processors located in or outside EU.

6. Obligations of Data Controller

6.1
Data Controller is obliged to provide all requests and instructions related to the performance of Contract Services to the Processor in writing.

6.2

As a diligent manager, the Data Controller is obliged to ensure the legality of the use of information assets that are the subject of the Contractual Service and over which the Processor does not have direct control or other potential influence in accordance with the contractual provisions.

7. Data Processor rights

7.1

Processor may suspend execution of Contractual Services if it suspects that execution of Data Controller's instructions violates applicable legislation, until confirmation or modification of the instructions. Processor is obliged to immediately forward the suspected breach of applicable law and its intention to terminate the performance of the Contract Services to Data Controller.

7.2

Processor may immediately terminate such activity in the event of suspicion of misuse or illegal use of information assets that are subject of the Contractual Services.

7.3

Processor may, for the performance of Contractual Services, conclude an appropriate agreement with sub-processors located or doing business in or outside EU to the extent and for a type of cooperation, as previously and in writing approved by Data Controller. If Data Controller does not set limits, the Processor may conclude an agreement with sub-processors of its own choice.

8. Obligations of Data Processor

8.1

The Processor is obliged to perform the Contractual Services only to the extent and for the purposes specified in the order of Contractual Services, General Conditions and according to written requests and instructions of the Data Controller.

8.2

The Processor will fulfill all the requirements of the Regulation in connection with the design and storage of audit trails in the performance of Contractual Services.

8.3

In accordance with the Regulation and good practice in information security, the Processor will continuously implement and upgrade all appropriate technical and organizational measures that ensure adequate protection of personal and other related data of individuals and the Data Controller, so that confidentiality, integrity, availability and resilience of systems and services will be ensured on a permanent basis.

8.4

The Processor will conclude appropriate contracts with the approved sub-processors in writing. The Processor is responsible for sub-processors to provide at least the same level of information security and protection of personal data as it is provided by itself.

8.5

At the receipt of an individual's request for the exercise of any right guaranteed by the Regulation, and if he can link the individual with the Data Controller based on information available to him, the Processor will transmit such request promptly and in writing to the Data Controller.

8.6

All employees and other persons involved in the provision of Contractual Services on the Processor's side, are bound to comply with the instructions and standards to be provided by the Data Controller and the Regulations (Articles 28, 29, 32).

8.7

All employees and other persons involved in the performance of Contractual Services on the Processor's side, are obliged to respect professional secrecy.

8.8

The obligation of professional secrecy is also valid after the termination of employment or other contractual relationship or the termination of cooperation between the Data Controller and the Processor.

8.9

The Processor will cooperate with the Office of the Information Commissioner in cases specified in the Regulation or based on a written request from the Data Controller.

8.10

After completion of Contractual Services, the Processor will hand over all received personal data collections to the Data Controller within 30 days at the latest

8.11

Unless otherwise requested by the Data Controller, the Processor shall permanently destroy all copies, residues or traces of personal data that have been subject of the Contractual Services and/or data which he has come into contact with during the performance of the Contractual Services in 60 days at the latest. The only exceptions are data, copies or other records the storage of which is required by laws or technical constraints relating to backup copies.

9. Handling of incidents

9.1

The Processor guarantees that, in accordance with the Regulation and good practices in information security, all technical and organizational measures are in place to ensure management and implementation of appropriate activities in the event of suspected or detected security incidents and/or loss of confidentiality.

9.2

Upon suspected or perceived security incidents and/or loss of confidentiality, the Data Controller and the Processor will take immediate action in accordance with Articles 33 and 34 of the Regulation.

9.3

In addition to carrying out all the activities foreseen in their internal regulations, the Data Controller and the Processor will notify each other, within a period of 72 hours, if they suspect or detect a security incident and/or loss of confidentiality.

9.4

The Data Controller and the Processor will inform each other about analyses of all circumstances related to detected security incidents and/or loss of confidentiality, and, based on these findings, they will improve and upgrade their practices and systems.

10. Validity of the Statement

10.1
New versions of this Statement completely replace the existing version.
10.2
The Data Controller and the Processor confirm that no provision of this Statement, the basic Contractual relationship, written requirements or instructions, shall relieve them of their individual duty to comply with the provisions of the Regulation and the responsibilities deriving therefrom.
10.3
In the event of disputes in connection with the security of personal data, the provisions of this Statement shall take precedence over the terms of the basic Contractual relationship.
10.4
In case of disputes, arising from this Statement, the court in Ljubljana shall be the competent court, using the laws of the Republic of Slovenia.
10.5
Invalidity or unenforceability of individual provisions of this Statement does not affect the validity and enforceability of other provisions of this Statement.
10.6
This Statement is accepted and binding also for any other contractual partner from the moment of submission or confirmation of his order, or at the latest from the moment of making the payment. For existing contractual partners, this Statement shall be valid from the moment of its publication.
10.7
This Statement is valid throughout the validity period of the basic Contractual relationship.

Milan, 05.11.2018

Giandomenico Sica
Executive President