# PIWIK PRO DATA PROCESSING AGREEMENT

*Updated August 10, 2021*

This Data Processing Agreement (this "Agreement") contains the terms and conditions that govern personal data transfers, hosting, and other related services provided by Piwik PRO (the "Services"). This Agreement shall be read together with the Master Services Agreement. The term "you", "your" includes any of your subsidiaries, affiliates and employees. BY ACCEPTING THESE TERMS OR BY USING PIWIK PRO SERVICES IN ANY MANNER YOU, THE ENTITY YOU REPRESENT AND ANY AFFILIATE OF SUCH ENTITY AGREE THAT YOU HAVE READ AND AGREE TO BE BOUND BY THIS AGREEMENT.

## Preamble

The Customer ordered the Piwik PRO Service, either by Purchase Order or by accepting the Master Services Agreement (both hereinafter referred to as "Main Agreement"). The Contractor shall collect, process and use personal data on behalf of the Customer in certain circumstances defined in the scope of the Agreement.

The parties to the Agreement wish to accommodate their mutual obligations in terms of legal data protection in accordance with the prerequisites of article 28 of the General Data Protection Regulation ("GDPR"), and therefore conclude the following agreement on commissioned data processing:

## 1. Definition

The following concepts have the meanings set forth below:

**Piwik PRO or Contractor** means Piwik PRO SA, ul. Św. Antoniego 2/4, 50-073 Wrocław, Poland, its subsidiaries and affiliated companies.

**Collection** has the meaning defined in article 4 no. 2 GDPR.

**Personal Customer Data** means any type of Customer data which are of a personal nature and which the Contractor collects, processes or uses within the

context of the agreement. “Personal data” has the meaning as defined in article 4 no. 1 GDPR which covers any information relating to an identified or identifiable natural person (hereinafter referred to as “Data Subject”); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

**Instruction** means any direction the Customer gives to the Contractor through which the Customer requests the execution of a certain action with reference to Personal Customer Data.

**The processing of personal data** has the meaning regulated in article 4 no. 2 GDPR.

**Usage/use of personal data** has the meaning regulated in article 4 no. 2 GDPR.

**Service** refers to the access to Piwik PRO Analytics Suite service provided by the Contractor free of charge or as part of the paid subscription.

**2. General**

2.1. Object of the agreement: This Data Processing Agreement is applicable to all activities connected to the contractual relationship of the parties, as part of which the employees or workers (employed on basis of a civil-law contract, freelancer) and/or as far as permissible under this agreement subcontractors of the Contractor collect, process or use the Customer’s personal data.

2.2. Scope, nature, purpose and duration of the commissioned data processing: The Piwik PRO Analytics Suite provides several modules that are internally connected and able to process information between each other. The service is used to analyze the use of websites by the Customer’s visitors, manage other marketing tools, personalize content viewed by the visitor, onboard any other data of the Customer and create audiences. Considering the above, Personal Customer Data shall be collected by Piwik PRO Analytics Suite based on profiles, events or comparable actions, regarding technical properties or activities of visitors to the Customer’s web pages or mobile applications. These Customer Data shall be evaluated by Piwik PRO to produce reports at different time intervals which may,

amongst others, include statements on the geographical origin, length of stay, interaction with the website or origin. The Contractor shall collect, process and use personal data he collects, processes or uses in the context of this Agreement on behalf of the Customer exclusively for fulfilling the purposes set out above.

The platform allows integration of tags of third party tools as well as creating an export of data to different third parties away from the scope of this contract and the area of responsibility of the Contractor. Moreover, the platform allows to import any other data that integrates with the data mentioned above. Therefore, it is within Customer's responsibility to fulfil country specific legal and data privacy regulations for each such use.

2.3. Data subjects: visitors of the Customer's web pages, web applications, native mobile applications, intranet portals (together hereinafter referred to as the "Customer's Services") and physical persons whose data was imported by the Customer in to the platform such as system users, end customers, employees, citizens or patients.

2.4. Type of data: Piwik PRO Analytics Suite collects data in the form of technical characteristics of the browser of the Customer's Services' visitor, activities on the Customer's Services, length of stay on the Customer's Services. The IP address of visitors of the Customer's Services is also collected. It is possible that any kind of data imported by the Customer can be processed on demand of the Customer. The Customer will immediately inform the Contractor if the imported data fulfills the requirements of article 9 GDPR (special categories of personal data). The Customer must make sure that data is collected on a lawful basis and are not processed without a need and a legal ground by the Contractor.

2.5. Data Storage: The collection and storage of said personal data by the Contractor takes place exclusively within a processing region. Piwik PRO offers the following data storage locations:

- EU West (Netherlands & Ireland) or
- DE Central (Germany) or
- US East (United States) or
- Southeast Asia (Singapore) or
- Any other as indicated by Piwik PRO in Purchase Order or Main Agreement

Piwik PRO ensures that the storage is located in **one** of the regions of choice. As part of the Services Piwik PRO may, from time to time, provide the Customer with support services which may in ordinary course of business constitute data processing (e.g. during a screen sharing session with Customer). Any such processing will take place in the European Economic Area. Any data collected during such support Service shall be immediately destroyed.

2.6. Term and Termination: As for the term and termination rights of this Agreement the provisions applicable of the Main Agreement shall apply. Termination of the main contract automatically leads to a termination of this agreement. With finishing the services provided by the Contractor or earlier, at the demand of the Customer, the Contractor is obliged to return the Customer all Customer's data files related to the contractual relationship and this commissioned data processing or to destroy them in accordance with applicable law with Customer's prior approval. Confirmation of the erasure or destruction must be presented to the Customer upon request. If any documents and data carriers related to the contractual relationship and this commissioned data processing is transferred to the Contractor by the Customer, the above shall apply as well.

**3. Rights and duties of the Customer**

3.1. Only the Customer shall be responsible for establishing the admissibility and lawfulness of the data processing, collection and use as well as observing the rights of the Data Subjects. This includes gathering and processing consents from Data Subjects.

3.2. The collection, processing and use of personal data within the framework of the contractual relationship and this Agreement take place exclusively according to the Instructions of the Customer (article 28 paragraph 3a GDPR).

3.3. The Customer shall issue Instructions about the processing of personal data via Customer portal.

3.4. The Contractor will process the Personal Customer Data in line with the Instructions provided by the Customer. However, if the Contractor believes an Instruction issued by the Customer constitutes a breach of data protection law, the Contractor shall immediately inform the Customer. The Contractor is entitled

to suspend the corresponding Instruction until it is confirmed or changed by the Customer.

3.5. The Customer is responsible for the accountability of the processing of Personal Customer Data and any measures taken in that respect. He will further take care of the portability of Personal Customer Data.

**4. Obligations of the Contractor**

The Contractor has the following obligations:

4.1. The Contractor processes personal data exclusively as agreed in this Agreement or as instructed by the Customer, unless the Contractor is legally obliged to perform a certain processing. If such obligations exist, the Contractor shall inform the Customer of this before the processing takes place, unless it is legally forbidden for the Contractor to do so.

4.2. The Contractor confirms that he is aware of the relevant general legal data protection regulations. He respects the principles of correct data processing and shall strictly observe confidentiality during the processing of the data.

4.3. The Contractor has appointed a data protection officer, who will carry out his or her activity in accordance with article 37 GDPR. The contact email of the data protection officer is the following: **gdpr@piwik.pro**

4.4. The Contractor shall only allow the collection, processing and use of personal data by personnel who have not been appropriately barred from the unauthorized collection, processing and data of personal data.

4.5. At the end of the Main Agreement, any of the Customer's user data shall also be deleted after any appropriate surrender of the data to the Customer (see section 2.6). The Contractor is entitled to keep any documentation it needs to prove that processing of the data has taken place in accordance with the order and regulations, in accordance with current legal storage times, after the end of the contract.

4.6. The implementation of and compliance with all technical and organizational measures necessary for this commission is regulated in **Annex 1.**

4.7. The Contractor shall regularly inform the Customer regarding the technical and organizational measures, and events that are significant for the security or confidentiality of the Personal Customer Data. He shall immediately communicate any disruptions or other irregularities during the handling of the Personal Customer Data or breaches of this Agreement to the Customer and agree on next steps. Only the Customer is liable to escalate data breaches to the regulatory authority and the data subjects. The Customer is liable for notification of the personal data breach to the regulatory authority in accordance with article 33 paragraph 1 GDPR and for the fulfilment of the Controller's obligation to respond to requests for exercising the data subject's rights laid down in chapter III GDPR. Therefore, he will decide whether a notification must be made to the regulatory authority and the data subjects, as applicable, because of the information made available to it by the Contractor regarding an incident. The Contractor shall provide comprehensive support for the Customer and immediately provide him with all the required information so that the Customer can fulfil its obligations to report both to the regulatory authority and to the Data Subjects, if applicable. Only the Customer is liable if he refrains from making a required report as per the above despite having been informed by the Contractor.

4.8. The Contractor may only issue Personal Customer Data to third parties or Data Subjects after obtaining prior consent from the Customer.

4.9. The Contractor shall inform the Customer immediately of inspection activities and measures by the regulatory authority or other third parties, if they have a relation to the commissioned data processing and Contractor can do so under applicable law.

4.10. The Contractor shall regularly carry out checks for the purpose of order control, in particular for the compliance with, and to make any necessary adjustments to regulations and steps for the fulfilment of this Agreement.

4.11. The Contractor shall inform the Customer immediately of any violations of the protection of personal data. Any cases for which there is justifiable suspicion of a breach must also be communicated. The Customer must be notified without undue delay after the Contractor becomes aware of relevant events, and notification must be made to the address given by the Customer.

**5. Technical and organizational measures**

5.1. The Contractor implemented the technical and organizational measures listed in **Annex 1** of this Agreement and shall maintain them during the term of this Agreement.

5.2. The technical and organizational measures are subject to technical progress and further development. In this regard the Contractor is authorized to implement alternative adequate measures. In these cases, the security level may not fall short of the measures established.

**6. Sub-contractual relationships**

6.1. The transfer of data-processing tasks by the Contractor, in the context of the activities agreed upon in the contract, to subcontractors, requires the prior notice to the Customer. Piwik PRO shall keep an up-to-date list of subcontractors as an Annex to this Agreement.

6.2. Supplementary services provided by third parties which the Contractor makes use of to support the execution of the Main Agreement are not to be understood as sub-contractual relationships within the meaning of this Agreement. These include for example communications services – including ticketing platform and mailing platforms, maintenance and user service, cleaners, inspectors or the disposal of data carriers. The Contractor is however obliged to fulfil contractual agreements suitably and in compliance with the law and take verification measures in order guarantee the protection and security of the Customer Personal Data, including when supplementary services are outsourced.

6.3. The sub-contractual data processing agreement must indicate an adequate level of protection comparable to that of this agreement. The Contractor is further required to check all requirements of article 28 of the GDPR are met with respect to involved subcontractors.

6.5. At present the subcontractors identified in **Annex 2** by their name, address and brief are occupied with the processing of personal data to the extent specified and are approved by the Customer.

**7. Rectification, erasure and blocking of data**

7.1. The Contractor may only rectify, erase or block the data collected, processed and used on behalf of the Customer according to instruction of the Customer. If a data subject applies directly to the Contractor for this purpose, the latter must immediately forward this request to the Customer.

7.2. The Customer shall check the request and inform the Contractor in writing whether it was justifiable or not and instruct the Contractor to proceed to rectify, erase or block.

7.3. The Contractor shall follow the relevant instructions of the Customer at all times during the term of this contract.

**8. Customer's control rights, contractor's cooperation duties**

8.1. The Contractor grants the Customer the right to carry out controls as agreed with the Contractor, during the Contractor's normal business hours or after making a prior appointment, or to allow third parties authorized by the Customer to carry out such controls. Upon demand, he shall provide the Customer with the relevant information. The result of these controls must be documented and provided to the Contractor.

8.2. The Contractor may also make a claim for remuneration for the facilitation of controls by the Customer.

8.3. Provided the Contractor correctly implements the agreed data protection obligations as envisaged under 8.3 of this contract, any checks should be based on sampling.

**9. Final clauses**

9.1. Annex 1 and 2 form a component of this Agreement.

9.2. Any changes and amendments to this Agreement and all its components require the written agreement of the parties. This is also applicable to the waiver of this formal requirement itself.

9.3. In the event of any inconsistencies the regulations of this agreement shall take precedence over the provisions of the main contract. If any sections of this

contract come out to be invalid or ineffective the effectiveness or validity of the remaining regulations within the contract shall remain unaffected.

**Signature section:**

| | |
|---|---|
| Customer:<br>By:<br><br>Name:<br>Position:<br>Date: | Contractor: Piwik PRO SA<br>By:<br><br>Name: Piotr Korzeniowski<br>Position: COO |

# Annex 1

**Technical and organizational measures**

The Contractor establishes the following technical and organizational measures and shall maintain them continuously:

1. **Confidentiality (Art. 32 par. 1 lit b GDPR)**

**1.1. Data Center**

Operator shall mean a Data Center operator which is a Subcontractor by the definition of this Agreement that specializes in the infrastructure delivery services.

| Domain | Practices |
|---|---|
| Organization of Information Security | **Security Ownership.** Operator has appointed one or more security officers responsible for coordinating and monitoring the security rules and procedures.<br>**Security Roles and Responsibilities.** Operator personnel with access to Customer Data are subject to confidentiality obligations.<br><br>**Risk Management Program.** Operator performed a risk assessment before processing the Customer Data or launching an Online Service.<br><br>Operator retains its security documents pursuant to its retention requirements after they are no longer in effect. |

| | |
|---|---|
| Asset Management | **Asset Inventory.** Operator maintains an inventory of all media on which Customer Data is stored. Access to the inventories of such media is restricted to Operator personnel authorized in writing to have such access.<br>**Asset Handling.**<br>● Operator classifies Customer Data to help identify it and to allow for access to it to be appropriately restricted.<br>● Operator imposes restrictions on printing Customer Data and has procedures for disposing of printed materials that contain Customer Data.<br>● Operator personnel must obtain Operator authorization prior to storing Customer Data on portable devices, remotely accessing Customer Data, or processing Customer Data outside Operator's facilities. |
| Human Resources Security | **Security Training.** Operator informs its personnel about relevant security procedures and their respective roles. Operator also informs its personnel of possible consequences of breaching the security rules and procedures. Operator will only use anonymous data in training. |
| Physical and Environmental Security | **Physical Access to Facilities.** Operator limits access to facilities where information systems that process Customer Data are located to identified authorized individuals.<br>**Physical Access to Components.** Operator maintains records of the incoming and outgoing media containing Customer Data, including the kind of media, the |

| | |
|---|---|
| | authorized sender/recipients, date and time, the number of media and the types of Customer Data they contain.<br>**Protection from Disruptions.** Operator uses a variety of industry standard systems to protect against loss of data due to power supply failure or line interference.<br>Component Disposal. Operator uses industry standard processes to delete Customer Data when it is no longer needed. |

| | |
|---|---|
| Communications and Operations Management | **Operational Policy.** Operator maintains security documents describing its security measures and the relevant procedures and responsibilities of its personnel who have access to Customer Data.<br>**Data Recovery Procedures.**<br>● On an ongoing basis, but in no case less frequently than once a week (unless no Customer Data has been updated during that period), Operator maintains multiple copies of Customer Data from which Customer Data can be recovered.<br>● Operator stores copies of Customer Data and data recovery procedures in a different place from where the primary computer equipment processing the Customer Data is located.<br>● Operator has specific procedures in place governing access to copies of Customer Data.<br>● Operator reviews data recovery procedures at least every six months. except for data recovery procedures for Azure Government Services, which are reviewed every twelve months.<br>● Operator logs data restoration efforts, including the person responsible, the description of the restored data and where applicable, the person responsible and which data (if any) had to be input manually in the data recovery process.<br>**Malicious Software**. Operator has anti-malware controls to help avoid malicious software gaining unauthorized access to Customer Data, including malicious software originating from public networks.<br>**Data Beyond Boundaries.** |

| | |
|---|---|
| | • Operator encrypts, or enables Customer to encrypt, Customer Data that is transmitted over public networks.<br>• Operator restricts access to Customer Data in media leaving its facilities.<br>**Event Logging.** Operator logs, or enables Customer to log, access and use of information systems containing Customer Data, registering the access ID, time, authorization granted or denied, and relevant activity. |

| | |
|---|---|
| Access Control | **Access Policy.** Operator maintains a record of security privileges of individuals having access to Customer Data.<br>**Access Authorization.**<br>• Operator maintains and updates a record of personnel authorized to access Operator systems that contain Customer Data.<br>• Operator deactivates authentication credentials that have not been used for a period of time not to exceed six months.<br>• Operator identifies those personnel who may grant, alter or cancel authorized access to data and resources.<br>• Operator ensures that where more than one individual has access to systems containing Customer Data, the individuals have separate identifiers/log-ins.<br>**Least Privilege.**<br>• Technical support personnel are only permitted to have access to Customer Data when needed.<br>• Operator restricts access to Customer Data to only those individuals who require such access to perform their job function.<br>**Integrity and Confidentiality.**<br>• Operator instructs Operator personnel to disable administrative sessions when leaving premises Operator controls or when computers are otherwise left unattended.<br>• Operator stores passwords in a way that makes them unintelligible while they are in force.<br>**Authentication.** |

| | |
|---|---|
| | • Operator uses industry standard practices to identify and authenticate users who attempt to access information systems.<br>• Where authentication mechanisms are based on passwords, Operator requires that the passwords are renewed regularly.<br>• Where authentication mechanisms are based on passwords, Operator requires the password to be at least ten characters long.<br>• Operator ensures that de-activated or expired identifiers are not granted to other individuals.<br>• Operator monitors, or enables Customer to monitor, repeated attempts to gain access to the information system using an invalid password.<br>• Operator maintains industry standard procedures to deactivate passwords that have been corrupted or inadvertently disclosed.<br>• Operator uses industry standard password protection practices, including practices designed to maintain the confidentiality and integrity of passwords when they are assigned and distributed, and during storage.<br>• Operator uses multi-factor authentication mechanisms to all systems related to the provision of the Services.<br>Network Design. Operator has controls to avoid individuals assuming access rights they have not been assigned to gain access to Customer Data they are not authorized to access. |

| | |
|---|---|
| Information Security Incident Management | **Incident Response Process.**<br>• Operator maintains a record of security breaches with a description of the breach, the period, the consequences of the breach, the name of the reporter, and to whom the breach was reported, and the procedure for recovering data.<br>• **Service Monitoring**. Operator security personnel verify logs at least every six months to propose remediation efforts if necessary. |
| Business Continuity Management | • Operator maintains emergency and contingency plans for the facilities in which Operator information systems that process Customer Data are located.<br>• Operator's redundant storage and its procedures for recovering data are designed to attempt to reconstruct Customer Data in its original or last-replicated state from before the time it was lost or destroyed. |

## Practices

### 1.2. Physical access control to Piwik PRO premises

The Contractor regulates access to the Piwik PRO premises by means of an access control system:

- The entrance doors are locked at all times and are unlocked by means of an electronic door lock
- An electronic card reader on a physical barrier at the entrance to the company premises.
- All persons must identify themselves additionally by means of a digital key (2nd authentication factor) to acquire access to the premises after business hours.
- Internal alarm system.

- Security and porters are available in the building 24/7. As well as the 24/7 video surveillance of the building.
- Loss of electronic cards must be reported immediately. If the electronic card is lost it is immediately blocked and will not enable access to the premises.

**1.3. Remote access control**

The following technical (password protection) and organizational (user master record) measures are deployed regarding user identification and authentication:

- Safe access link and up-to-date technology is employed for authentication in order to regulate access to the productive system and support tools. The following user groups are granted access by the Contractor:
- Administrators: configuration, monitoring and maintenance
- Developers: source code deployment, maintenance of source code
- Support: customer support including access to the instance User Interface
- Direct access to the server is only possible from the Contractor's (IP-restricted) network secured by means of a "Virtual Private Network" connection.
- Each user receives their own VPN certificate. The authentication of the user is ensured by means of a 4096-bit key pair (private and public) in which the public part of the key is saved on the server and the user holds the private part. This procedure ensures that the productive system is protected against access by unauthorized persons.
- To perform web-based administrative functions, users must establish a VPN connection
- Administrators must additionally identify themselves by entering a password. Real-time notification about incorrect password attempts appears. Access is additionally limited by SSH key from white-listed IP addresses.
- Access to the database is exclusively withheld by the group of administrators.
- Developers only receive limited access for maintenance of the source code / maintenance of the application and provision of new functionalities.
- Implemented monitoring that records the activities of the individual users. Wrong entry of passwords upon access to the productive system are logged and reported to the Contractor in real time. Any changes to user accounts, creation of users and/or user groups, changes of rights, user

rights in the database, changes to the firewall rules and password changes are logged.

### 1.4. Access control to application

Interface access, through username and password, is limited to the Customer or persons authorized by it and in addition to accordingly-authorized employees of the Contractor, by means of username and password. Access to the application interface can be limited to specific IP addresses.

The Contractor shall issue an authorization to each employee or other person who shall be admitted to the data processing and keeps records of persons authorized to data processing. Each employee or other person admitted to the data processing by the Contractor has become familiar with the regulations concerning data protection and is obliged to keep the data and security means thereof confidential during the employment/contractual relationship and after it has ended.

## 2. Integrity (Art. 32 par. 1 lit b GDPR)

### 2.1. Transport and transfer checks, data carrier and user controls

The Contractor has established the following transport, transfer, data carrier and user controls, which ensure that personal data cannot be read, copied, altered or removed by unauthorized parties in the course of electronic transmission or during transportation or recording on data carriers, and that it is possible to examine and establish to which bodies personal data are to be transferred using data transmission equipment:

- The web application is reachable exclusively over HTTPS.
- Isolated internal communication (separate virtual network)
- Database with no direct access
- Firewalls configured to deny incoming connections by default
- Detection of suspicious/malicious activity

Access to the Piwik PRO Analytics Suite is subject to effective access controls which are described in more detail in Section 1.4 of this Annex 1. Transfer is only permitted upon access by a secure SSL (“Secure Socket Layer”) connection.

### 2.2. Input control

The transmission of the personal data takes place by means of implementation of the corresponding tracking code by the Customer. Every tracking code has an unambiguous allocation for a profile / a website which was previously created by a person with authorized access.

Access or alteration of the collected data is subject to effective access mechanisms and are logged correspondingly.

**3. Availability and capacity (Art. 32 par. 1 lit b GDPR)**

**3.1. Availability control**

The Contractor has implemented a monitoring system which will supervise the firewall and switches, the server answer time, DNS answer time, webpage loading time, the total number of requests, physical servers' reliability and HTTP error codes that occur. Every unauthorized access of files, directories or programmed code is detected. The Contractor employs a combination of redundant systems for load balancing and backup solutions so that data can be recovered at any time in the event of a failure.

The Contractor has established availability checks, which ensure that all system and application components are working without any malfunctions.

**3.2. Backup policy**

Redundant storage and its procedures for recovering data are designed to attempt to reconstruct Personal Customer Data in its original or last-replicated state from before the time it was lost or destroyed.

Types of data to be backed up:

- Database data
- Client HTTP access logs
- System configuration

Backup media:

- Redundant storage attached to dedicated backup server close to production servers

- Off-site storage – redundant storage attached to dedicated backup server located in a different geographic location

Retention policy for all types of backups (periods):

- Keep daily backups for – 8 days
- Keep weekly backups for – 5 weeks
- Keep monthly backups for – 2 Months

Access to backups:

- Restricted to specific IP
- Users must establish VPN connection

Backup monitoring

- Size
- Execution time

**3.3. Recoverability**

The Contractor employs a combination of redundant systems for load balancing, databases and backup solutions so that data can be recovered at any time in the event of a failure Strict backup policy and procedure ensure that data can be restored with minimum granularity.

**3.4. Data integrity**

The guarantee that stored personal data cannot be damaged by system malfunctions.

The Contractor has installed a daily check which verifies the consistency of the data. Moreover, the system is scanned and checked every day for ‘malware’ and ‘rootkits’.

**3.5. Data separation control**

Each customer has all reporting data stored in a separated database. Actual data storage is separated from the tracking data receival endpoint (frontend machine). This means the storage itself is not exposed to the internet.

**4. Procedures for periodic review, assessment and evaluation (Art. 32 par. 1 lit d GDPR)**

Periodic review, assessment and evaluation of Technical and Organizational measures are being performed according to the audit schedule required for information security certification ISO/IEC 27001:2013.

# Annex 2

## Subcontractors

For the processing of data on behalf of the Customer, the Contractor employs services of third parties who process data on its behalf (“subcontractors”).

The following company/companies are subcontractors:

1. Microsoft Ireland Operations Limited, South County Business Park, Leopardstown, Dublin 18, Ireland. (“Operator” according to Annex 1)