PERSONAL DATA PROTECTION

1.1 – **Processing of personal data as data controller:** when the Service Provider processes personal data under this Contract as data controller, it undertakes to comply with the applicable data protection legislation, in particular the French Data Protection Act of 6 January 1978 as amended and Regulation (EU) 2016/679 of 27 April 2016 (hereinafter the "European Regulation").

1.2 – **Definitions of Personal Data (PD):** any information relating to an identified natural person or a person who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more elements specific to him.

Data subject: natural person to whom the data subject to the processing of PD relates.

Data Controller (DC): the entity that determines the purposes and means of processing PD. Data processor: the natural or legal person, public authority, agency or other body that processes PD on behalf of the Data Controller.

Data processing: any operation or set of operations relating to PD, regardless of the process used, and in particular the collection, recording, organisation, storage, adaptation or modification, extraction, consultation, use, communication by transmission, dissemination or any other form of provision, reconciliation or interconnection, as well as blocking, erasure or destruction.

1.3 – **Identity of the Personal Data Controller**

MITWIT MWPI, whose registered office is located at 58 Avenue de la Grande Armée 75017 PARIS France

MITWIT GARES, whose registered office is located at 4 place Louis Armand 75012 Paris France

NCI, whose registered office is located at 143 avenue Louise Box 4 1050 Brussels Belgium

Multiburo Mitwit (Suisse) SA, whose registered office is located at 1, Rue de la Cité 1204 Geneva Switzerland

Means the Service Provider and the data controller, the purpose of the processing being described below.

1.4 – **Purposes of personal data processing**

The privacy policy below applies if the Service Provider acts as data controller for the processing of personal data received from the User under this Contract.

If, as a User, you share the personal data of employees, agents or other third parties with the Service Provider, you are required to inform your employees, agents or other third parties who benefit from the Service Provider's offer of this privacy policy before providing their personal data to the Service Provider. For any questions or procedures relating to your personal data, we invite the data subject to contact our data controller and our data protection officer (Mr Jérôme Zatti) on dpo@mitwit.com.

The Service Provider implements PD processing for the purposes envisaged below:

Purpose	Categories of data subjects	Categories of personal data processed	Categories of recipients of personal data
Conclusion and management of the Contract (Management of the pre-contractual relationship and contracting, preparation of accounts and invoicing, collection of unpaid amounts, creation of a user profile), including the collection of data relating to the identity of the user and the user's	- Natural person user - In the case of a User legal entity, natural person(s) representing the User - The User's employees benefiting from the	- Identification data: last name, first name, e.g. membership card no., identity card of the User or his representative - Business data: business email address, business postal address (if Beneficiary), business telephone number, job function/position, company	- authorised internal departments of the Service Provider (sales department, finance department and legal department) - data processors or partners that need to know about the conclusion/management of the Contract (bank(s) of the Service Provider and the Beneficiary, banking partners for

Employees pursuant to article 6.1 b of the GDPR	Service Provider's services - Authorised personnel of the User (accountant etc.) interacting on behalf of the Beneficiary with the Service Provider	- Economic and financial data: data relating to transactions (invoices, bookings, etc.) and bank details depending on the payment method chosen (bank details or SEPA mandate – if credit card, the number is not processed by the Service Provider but by its banking partners) - Data on the use of the Service Provider's Spaces and Services: printer logs for invoicing	payment verification or transaction management, invoicing and accounting management solutions) - IT service providers (data hosting providers) – if necessary, certain regulated professions (e.g. lawyers)
Performance of the services provided for in the Contract (management of bookings of the Service Provider's Spaces and Services; provision of the Spaces; management of complaints and assistance; physical reception; provision of IT/telecommunications	Natural person user - In the case of a User legal entity, natural person(s) representing the User - The User's employees	- Identification data: last name, first name, e.g. membership card no., identity card of the User or his representative - Computer data: IP address and Wi-Fi login details - Economic and financial data: billing	- authorised internal services of the Service Provider (operations, sales and finance services) - IT service providers (host or technical service provider) - data processors or

equipment and systems), excluding the services referred to in Purpose 3, pursuant to article 6.1 b of the GDPR (performance of a contract or precontractual measures) when the Data Subject is the User or, pursuant to article 6.1 f of the GDPR (legitimate interests of the Service Provider to comply with its contractual commitments to the User) when it concerns Data Subjects who are not parties to the Contract (User's Employees etc.).	benefiting from the Service Provider's services - Authorised personnel of the User (accountant etc.) interacting on behalf of the Beneficiary with the Service Provider -Natural person(s) invited by the User (or by the Employees of the User) to a site	address if User and information relating to the payment order - Data on the use of the Service Provider's Spaces and Services: office preferences, calendar of reserved Spaces or rooms, communications via our Services - Location data on the Service Provider's website and application (subject to consent pursuant to article 6.1 of the GDPR) to offer Spaces to the user based on its location	partners that need to know about the conclusion/management of the Contract (if applicable, partner or manager of the Space concerned by the order) - service providers (banking partners, online booking system, etc.) - if necessary, certain regulated professions (e.g. lawyers)
Management of the business relationship (sending newsletters, emailing of information and targeted communications, commercial offers, quotes, sales canvassing, assessment of customer satisfaction	- Natural person user - In the case of a User legal entity, natural person(s) representing the User	- Identification and business contact data: last name, first name, job function/position, company, business email, business telephone number, member number.	- authorised internal departments of the Service Provider (marketing department, sales department) - IT/telecommunications service providers (data hosting or IT service provider)

and experience, establishment of attendance statistics) pursuant to article 6.1 a of the GDPR (consent of the Data Subject and for newsletters) or article 6.1 f of the GDPR (legitimate interest of the Service Provider or a third party to carry out promotional, marketing or sales canvassing operations on these services, to analyse the needs of the Beneficiaries or its Employees in accordance with the Service Provider's corporate purpose).	- The User's employees benefiting from the Service Provider's services	- IT and web browsing data: e.g. IP address - Data on the use of the Service Provider's Spaces and Services: office preferences, calendar of booked Spaces or rooms, communications via our Services, access logs using badges, anonymous statistics for counting individuals from video surveillance systems, your opinions, recommendations, your questions/comments about the Spaces or Services	- data processors or partners that need to know about the conclusion/management of the Contract – service providers (e.g. email solutions, gym, surveys, etc.) or third-party advertising partners - if necessary, certain regulated professions (e.g. lawyers)
<u>Security of people, premises, information systems and property</u> (Physical access control by badge system, visitor keys or registers; accounting and control of the occupancy rate and flows; logical access control, management and security of access to the various applications of the IS; management,	- Natural person user - In the case of a User legal entity, natural person(s) representing the Beneficiary – Employees of the Beneficiary benefiting	- Identification and business contact data: last name, first name, job function/position, company, membership card no., identity card for verification - Computer data: login credentials for the website or application, computer	authorised internal departments of the Service Provider (operations department, site manager, IT department) - IT/telecommunications service providers (hosting company or technical service provider) - data processors, partners or service providers relating to security (e.g. security and

identification of fraud and security of the Wi-Fi network) pursuant to article 6.1 b of the GDPR primarily (performance of a contract or pre-contractual measures) and article 6.1 f of the GDPR (legitimate interest of the Data Controller to ensure the security of persons, information systems and property on its premises) on a subsidiary basis, excluding video surveillance (see below)	from the services of the Service Provider - Authorised personnel of the User (accountant, etc.) interacting on behalf of the User with the Service Provider - Natural person(s) invited by the User (or by the User's Employees) to a site of the Service Provider	data on devices (IP address etc.), access logs for IS applications, network (Wi-Fi or internal network) and printers - Data on the use of the Spaces: badge access logs	guarding company, IT support) - if necessary, certain regulated professions (e.g. lawyers)
<u>Corporate reorganisation</u> in respect of the legitimate interest of the Service Provider pursuant to article 6.1 f of the GDPR, including in the form of an assignment, merger or acquisition, sale or transfer of business or assets.	Natural person user - In the case of a User legal entity, natural person(s) representing the User	- Civil status and identification data: e.g. last name, first name – Business data: e.g. business email address, business postal address, business telephone number, capacity to act/functions	- authorised internal services of the Service Provider - IT service providers - In the context of due diligence, potential sellers or buyers and their advisors

(optional) Registered address of the Beneficiary: under the legal obligation of the Service Provider pursuant to article 6.1 c of the GDPR, to enable the Service Provider to comply with the obligations of article R. 123-168 of the French Commercial Code and ensure the collection of necessary data, the management, processing and monitoring of beneficiaries with registered address (file of supporting documents, information to the commercial court, communication to court bailiffs, list of persons with registered address, anti-money laundering, etc.).	- Natural person user - In the case of a User legal entity, natural person(s) representing the User	Civil status and contact data: e.g. last name, first name, telephone number and postal address, as well as corresponding supporting documents - Business data: e.g. business email address, business postal address, business telephone number, functions	- authorised internal services of the Service Provider - data processors or partners that need to know about the conclusion/management of the Contract (e.g. IT service providers hosting the data) - the recipients mentioned in article R. 123-168 of the French Commercial Code (clerk of the Commercial Court; bailiffs; tax centre and the competent social security contribution collection bodies) - if necessary, certain regulated professions (e.g. lawyers) Where necessary, it is specified that the Service Provider is authorised to disclose the aforementioned personal data when such data must be disclosed as a result of a judicial or administrative injunction or when its disclosure is necessary for the Service Provider to ensure its defence in the context of legal or administrative proceedings. The collection of data is

			limited to the information necessary to accomplish the purposes described below. Mandatory data are indicated as such in the collection forms.

1.5 Processing of personal data as a processor

Insofar as the Service Provider processes personal data as a processor on behalf of the User acting as data controller in the context of the provision of its services, the Service Provider shall process such personal data in accordance with the provisions set out below.

The processing generally concerns identification data, data relating to personal characteristics and data relating to employment and profession of (i) the User, (ii) its employees or agents benefiting from the services, and (iii) the User's clients or suppliers and their employees or agents, for the purpose of providing the services covered by this Contract. The Service Provider shall only process the personal data referred to in this article for the duration of the Contract, unless required to do so by Union law or applicable national law.

In the context of such processing, the Service Provider, acting as processor, shall:

– process the personal data only on the basis of the User's documented instructions set out in this Contract or elsewhere, including any transfer of personal data to a third country, unless required to do so by Union law or applicable national law, in which case the Service Provider shall inform the User prior to the processing of such legal requirement, unless such law prohibits such notification for important reasons of public interest;
– ensure that persons authorized to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
– implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, taking into account in particular the risks of processing resulting from destruction, loss, alteration, disclosure of, or unauthorized access to personal data, and ensure that any natural person acting under the authority of the Service Provider and having access to personal data shall not process them except on

instructions from the User, unless required to do so by Union law or applicable national law;
– taking into account the nature of the processing, provide the assistance requested by the User regarding its obligation to respond to requests from data subjects exercising their rights under the applicable data protection legislation, by means of appropriate technical and organizational measures, insofar as possible;
– taking into account the nature of the processing and the information available to the Service Provider, assist the User in complying with its obligations under the applicable data protection legislation with regard to the security of personal data, the notification of a personal data breach to the supervisory authority and, where applicable, to the data subjects, the carrying out of data protection impact assessments, where necessary, and the prior consultation with the supervisory authority. If the Service Provider becomes aware of a personal data breach covered by this article, it shall inform the User without undue delay by email using the contact details set out at the beginning of this Contract;
– at the choice of the User, after the provision of the services, delete or return all personal data to the User and delete existing copies, unless retention of such personal data is required by Union law or applicable national law;
– make available to the User all information necessary to demonstrate compliance with the obligations set out herein and contribute to audits, including inspections, conducted by the User or an auditor mandated by the User. This audit right of the User is limited to one audit every two years, except in the case of a serious security incident involving the User's personal data or if the User is required by a supervisory authority to carry out such an audit.

Where the Service Provider engages another processor, the following conditions shall apply:

(i) The User expressly authorizes the Service Provider to engage other processors, in which case the Service Provider shall inform the User in advance of any intended changes concerning the addition or replacement of other processors. The User may object to such changes within two weeks of notification by email to dpo@mitwit.com.

(ii) Where the Service Provider engages another processor to carry out specific processing activities under this Contract on behalf of the User, the Service Provider shall impose by contract on that other processor the same data protection obligations as those set out in this article. If the other processor fails to fulfil its obligations under the European Regulation, the Service Provider shall remain liable to the User for the performance of those obligations by the other processor, without prejudice to the other provisions of this Contract.

1.6 Information and rights of data subjects

In accordance with the GDPR, each Data Subject has the following rights:

1. Right of access: you may request access to the personal data we hold about you and to certain information about how it is processed. In some cases, and upon your request, we may provide you with an electronic copy of your data;
2. Right to rectification: you may request the rectification of any inaccurate or incomplete data concerning you. You must then demonstrate why such information is incorrect;
3. Right to restriction of processing: in certain circumstances, restriction of processing is possible. You may make this request at any time and we will decide on the follow-up;
4. Right to object: you may object to any processing based on our legitimate interest, on grounds relating to your particular situation and, in any case, when we send you marketing communications;
5. Right to erasure: in certain circumstances, you may request the deletion of your personal data. Where we determine, in accordance with the law, that your request is admissible, we will delete your personal data as soon as possible;
6. Right to portability: in certain circumstances, you may request that we provide you with your personal data in a commonly used and machine-readable format. If technically possible, you may also require that we transmit your data to another data controller;
7. Right to withdraw your consent: to the extent that the processing of your personal data is based on your consent, you may withdraw it at any time;
8. Right to formulate instructions relating to the retention, erasure and communication of your personal data after your death.

It is expressly agreed that the User guarantees to transmit to the natural persons acting on its behalf under the Contract, to its Employees benefiting from the services, as well as to persons invited by it or by its Employees, the information relating to the processing of personal data carried out by the Service Provider concerning them, their rights over such processing, and how to exercise them, in accordance with Articles 13 and 14 of the GDPR.

To exercise these rights or for any question regarding the processing of personal data in this context, the Service Provider may be contacted:

– via the rights request form available at the bottom of the page
– by electronic means: dpo@mitwit.com
– by postal mail (we recommend sending by registered letter):

MWPI: 58 Avenue de la Grande Armée 75017 PARIS France
MULTIBURO GARES: 4 place Louis Armand 75012 Paris France
NCI: 143 avenue Louise Box 4 1050 Brussels Belgium
MULTIBURO SA: 1, Rue de la Cité 1204 Geneva Switzerland

To enable the Service Provider to verify the identity of the Data Subject, the Data Subject may be asked to attach an identity document in PDF format to the email, or a photocopy of an identity document in the case of postal mail.

1.7 Data retention

The above-mentioned personal data is retained for as long as necessary to achieve the purposes for which it was collected.

To determine the appropriate retention period for personal data, the Service Provider considers the amount, nature and sensitivity of the personal data, the risk of unauthorized use or disclosure of the personal data, the purposes for which it is processed, and its legal obligations.

After this period, personal data is deleted or archived in accordance with legal and regulatory requirements.

1.8 Security of personal data processing

The Service Provider undertakes to implement appropriate technical and organizational security measures (such as periodic review of access rights, password protection, access and incident logs, regular data backups, antivirus software and firewalls, penetration tests, physical locks, etc.) to ensure the security of personal data and to protect them against any alteration, accidental or unlawful destruction, damage, loss, disclosure or access by unauthorized persons.

Furthermore, the Service Provider ensures that Sub-processors, when they may have access to personal data, are chosen based on the information and guarantees they provide regarding data protection.

The Service Provider also conducts audits to verify the compliance of such providers with their commitments. Access to personal data is granted only to authorized employees of the Service Provider, for the purpose of performing their professional duties, and such employees are subject to a confidentiality obligation.

It is also the responsibility of the User, the persons acting on its behalf, the User's Employees, as well as persons invited by them, to protect the confidentiality and security of their data, particularly when transmitting data over the Internet, and to follow good IT practices when using the Service Provider's website or application, or its IT systems. For further information, the ANSSI Guide to Good IT Practices can be consulted.

Privacy protection is everyone's responsibility. Any risks or security incidents (e.g. unauthorized entry into premises, loss of a laptop, phishing email, computer hacking) should be reported to the Service Provider as soon as possible, to give the Service Provider the best chance of preventing or reducing risks.

1.9 Transfer of personal data outside the EU

The recipients of personal data are mainly located within the European Union but may also be located outside the EU. In the latter case, if the country does not have an adequacy decision from the European Commission ensuring an adequate level of protection, the Service Provider takes the necessary security and legal measures to ensure the security and integrity of the transferred personal data and to ensure a sufficient and appropriate level of data protection in accordance with the requirements of the GDPR, through the conclusion of Standard Contractual Clauses.

1.10 Video surveillance

In application of Article 6.1 f of the GDPR (legitimate interest of the Service Provider), the common areas and the surroundings of certain Service Provider sites may be subject to video surveillance systems in order to ensure the security of persons, premises and property.

The rights of Data Subjects and the procedures for exercising them are the same as those mentioned above in this article.

More generally, the entire video surveillance system is managed in accordance with the rules and recommendations issued by the CNIL.