Rules of Operation of CE Colo and DC7 Data Centres

1. Recitals

1.1. These Rules of Operation (hereinafter the "Rules of Operation"), issued by CE Colo Czech s.r.o., with its registered office in Prague 10, Nad Elektrárnou, 1428/47, post code: 106 00, company ID: 241 97 327, registered in the Commercial Register maintained by the Municipal Court in Prague under file no. C 187768 (hereinafter the "Provider"), stipulate the conditions of operation of the Provider's data centres located at Nad Elektrárnou 1428/47, Prague, and K Pérovně 1616/2, Prague (hereinafter jointly the "Data Centre").

1.2. The conditions or, more precisely, the rights and obligations stipulated by the Rules of Operation are binding on the Provider, the Customer and any persons authorised by the Customer or the Provider to enter the Data Centre (or, more precisely, to perform the activities, exercise the rights and fulfil the obligations connected with the Data Centre).

1.3. Wherever the term Customer is used in these Rules of Operation, this also means any person authorised by the Customer to enter the Data Centre or, more precisely, to perform the activities, exercise the rights and fulfil the obligations connected with the Data Centre. This also means any person entering and performing activities in the Data Centre along with the Customer and/or with a person authorised to enter the Data Centre (e.g., a supplier of the Customer), with the exception of the provisions from the nature of which it follows that the relevant right or obligation can apply exclusively to the Customer. The rights and obligations specified for the Customer are also binding on any person authorised by the Customer to enter the Data Centre or, more precisely, to perform the activities, exercise the rights and fulfil the obligations connected with the Data Centre or a service of the Provider used there, without this being expressly specified, with the exception of those rights and obligations that can apply solely to the Customer.

1.4. Wherever the term Provider is used in this document, this also means any person authorised by the Provider to enter the Data Centre or, more precisely, to perform the activities, exercise the rights and fulfil the obligations connected with the Data Centre, with the exception of those provisions from the nature of which it follows that the relevant right or obligation can apply solely to the Provider.

1.5. The Data Centre will be also referred to in the Rules of Operation below as the premises, the site or the Data Centre.

1.6. For the purposes of the Rules of Operation, the Help Desk means the monitoring team of the Provider's Data Centre.

1.7. For these purposes, the Agreement means the particular Data Centre Service Agreement concerning, *inter alia*, the provision of technological space in the Data Centre or, if applicable, other services provided in the Data Centre, entered into between the Customer and the Provider, especially the Customer Order Form, as an annex to this Agreement.

2. Security – Entry to the Data Centre

2.1. The Data Centre is secured against entry by unauthorised persons in a number of ways. One of the Data Centre's security measures is the specification of the persons holding the "Access Permission" (entry authorisation) to access the technological areas of the Data Centre under the conditions defined below. The persons holding the "Access Permission" with no further check required (the Access Permission is non-transferrable) are as follows:

- The Provider's employees operating the service and the Help Desk;
- Tenants of the office space;
- Other authorised employees of the Provider; and
- Individuals providing services to the Provider (e.g. building security, reception and cleaning services).

2.2. The persons holding the "Access Permission" with a further check required are divided as follows:

- Provider's suppliers;
- Customer's authorised persons – individuals included in the authorised persons list supplied by the Customer.

2.3. Each of the persons in the above groups is assigned one of the following categories:

- Unlimited access (24x7x365);
- Temporary access;
- Escorted access;
- Unescorted access;

2.4. The persons who hold the "Access Permission" are included in the authorised persons list (a form of this list is attached as an annex to these Rules of Operation and forms an integral part of the Rules of Operation). The

authorised persons list also contains a list of the persons with the specification of their right to make changes in the authorised persons list. The individual authorisation levels are as follows:

- Level 1 – list administrator – the person allowed to authorise permanent and one-time access and to make changes of the levels in the list (Level 1 + 2 + 3);
- Level 2 – the person allowed to make changes in the permanent access list (list of authorised persons with permanent access permission) and authorise one-time access;
- Level 3 – the person allowed to authorise one-time (temporary) access based on an e-mail sent to helpdesk_cz@cecolo.com.

2.5. Entry to the technological space of the Data Centre is only permitted with the knowledge and prior consent of the Help Desk staff. Each person must report his/her entry to and exit from the technological space to reception. The Customer's authorised persons lists containing a specification of the scope of their access permission are saved in electronic form and are accessible to the Help Desk staff and reception staff of the Data Centre. The consent is granted by the issuance and activation of the access card.

2.6. If the Customer requests temporary access of other persons not included in the authorised persons list, the Customer's person authorised to the approve temporary access of other persons on behalf of the Customer must notify the Help Desk thereof by e-mail (helpdesk_cz@cecolo.com) sent from the contact addresses agreed in advance. Such notification must contain, at least, the identification details of the relevant person (namely the full name and the number of the official identity document) and the period of entry of such person to the technological space of the Data Centre. Subsequently, the authorised person must authorise the request submitted in this manner via the access system web interface. Without the consent verified in this manner, the person who is not included in the Customer's authorised persons list will not be permitted entry to the technological space of the Data Centre. Permanent changes in the Customer's authorised persons list may be made by the list administrator either via the access system web interface or they must be made by e-mail (helpdesk_cz@cecolo.com) sent from the agreed contact addresses (or, more precisely, by the Customer's persons authorised to do so).

3. Key and Access Card Management

3.1. The conditions of use of the electronic chip cards, PINs and biometric identifiers that serve for entry to the technological space of the DC7 Data Centre are regulated in the annex to these Rules of Operation titled Access Rules.

3.2. The electronic chip card intended for entry to the technological space of the Data Centre is always issued by the reception staff before entry. The keys necessary for the entry to the premises are subsequently issued by the Help Desk staff, security staff or an automated system. The keys and electronic chip cards must always remain in the Data Centre and must not be taken outside the Data Centre premises. The keys and electronic chip cards are labelled individually and listed in the logbook for key and electronic chip card management. The logbook contains the following records:

- Which keys have been lent;
- Date and time of lending the keys;
- Name of the person taking over the keys, including identification of the Customer for whom that person performs the activity in the Data Centre;
- Signature, telephone number and ID card (passport) number of the borrower of the keys;
- Date and time of return of the keys.

3.3. Access to the technological space of the Data Centre is only possible with an electronic chip card or its equivalent, issued by the reception staff. The Data Centre reception (or the Help Desk) staff will also issue a visitor card to the relevant person who holds the "Access Permission" with a further check required. Each person who holds the "Access Permission" with a further check required must wear the visitor card in a visible place for the entire period of the visit and must present himself/herself with that visitor card at the request of the Provider's employees.

3.4. In case of the loss of the electronic chip card, the Customer is obliged to pay to the Provider a contractual penalty of CZK 500.

3.5. In case of the loss of a key, the Customer is obliged to pay to the Provider a contractual penalty of CZK 7,000.

4. Rights and Obligations of the Customer

4.1. The Customer may access the Customer's reserved (leased) space and may operate his/her own equipment and the equipment of his/her customers there, including the installation and deinstallation of such equipment. The Customer may not enter any areas outside the Customer's reserved (leased) space and the areas necessary for access to such reserved (leased) space. It is prohibited to perform any installations, interfere with the technology of other persons, open the (antistatic) double floor and interfere with the Data Centre infrastructure or perform any

other activities outside the Customer's reserved (leased) space. The Customer may not connect any further extension cables to existing power strips.

4.2. It is prohibited to bring any items releasing dust and dirt or any food or liquids into the technological space or consume any food or liquids there. After completing work, the Customer must clean up any waste caused by his/her activities, including packaging, without any delay. It is strictly prohibited to store any packaging in the rack (cage) area. The Customer must keep the assigned space in a proper technical condition, i.e. in a condition intended for the proper provision of the Data Centre service, and in a condition in which the technological space was handed over to the Customer by the Provider.

4.3. For security reasons, the Data Centre premises and the movement of persons on these premises are monitored using a CCTV and security system 24x7 (in relation to this, see Article 8 of these Rules of Operation).

4.4. Any person entering the technological space must use the Provider's shoe covers located at the entrance to the technological space.

4.5. The Customer acknowledges and agrees that only the persons who (or whose personal data) are included in the authorised persons list that must be delivered by the Customer to the Provider or who are included in the authorised persons list, who have been assigned the means necessary for entry to the location (card, PIN, biometrics) and who received appropriate advice may enter the site; see the form attached to these Rules of Operation). The Customer may unilaterally change these persons in writing by delivering a notice to the Provider. The Provider collects and processes those data for the purpose of performing the relevant Agreement/Customer Order Form, especially for the purpose of allowing entry to the location solely to the authorised persons, and records the data on the persons authorised to enter the Data Centre in internal lists, i.e. the Access Lists (in relation to this, see Article 8 of these Rules of Operation).

4.6. If it is necessary that any other person who is not listed in the list of the persons authorised to enter the Data Centre (e.g., a supplier of the Customer) enters the Data Centre along with the Customer and/or with a person authorised to enter the Data Centre and performs activities in the Data Centre, the person authorised to enter the Data Centre must allow this in the list of the persons authorised to enter the Data Centre. One-time unescorted access will be governed by paragraph 2.6 of these Rules of Operation. Furthermore, the Customer or the person authorised to enter the Data Centre must make such person acquainted with the obligations resulting for him/her from his/her entry to the Data Centre, or more precisely, with the Rules of Operation. The Customer is liable for the performance of the obligations by such person and is liable for any damage resulting from the breach of obligations arising for that person from the Rules of Operation or any other document. For this purpose, the Provider will put up the Rules of Operation in the Data Centre so that the relevant person can read them.

4.7. The Customer is obliged to make the persons authorised to enter the Data Centre or any other persons entering the Data Centre along with the Customer or with a person authorised to enter the Data Centre acquainted with the conditions stipulated by the Rules of Operation (including any annexes thereto) and acknowledges that the Customer is liable for any breach of the conditions of the Rules of Operation and/or the Agreement (or, more precisely, for any damage incurred in connection therewith) committed by the persons authorised to enter the Data Centre or by any other persons entering the Data Centre along with the Customer or with a person authorised to enter the Data Centre, and, furthermore, the Customer is liable for any damage resulting from the actions or omissions of persons who are not authorised to enter the Data Centre but to whom the Customer allowed entry to the Data Centre.

4.8. The Customer must report any loss of the access card and/or key to the Help Desk without any delay, specifying the card and/or key number. The Customer bears full liability for any damage connected with such loss; this will in no way prejudice the Provider's right to the payment of the contractual penalty pursuant to paragraphs 3.4. and 3.5. of the Rules of Operation.

4.9. The Customer must not interfere with (or handle) any technology and/or equipment of the Provider or third parties that is located in the Data Centre.

4.10. When visiting the Data Centre, the Customer must comply with the security, safety and fire regulations of the Provider and/or owner of the site and must comply with any additional instructions that may be provided by the Provider's employees, particularly by the instructions from the Help Desk. The Customer may not enter any areas outside the reserved space in which his/her equipment is located in the assigned rack/cage.

4.11. The Customer may only disconnect his/her equipment from the 230V power supply within the particular rack/cage and may only do so by disconnecting the power supply cable of the equipment. In other cases where the disconnection of the equipment from the power supply requires a qualified person (such as clamps or screws/lugs), the Customer must contact the Help Desk in advance, and the Help Desk will disconnect the Customer equipment from the power supply at the agreed time. Each such disconnection will be recorded in a logbook (ticket), stating the date, time, person's name, designation of the rack/cage, power distribution unit and circuit breaker, and the reason for handling the power distribution unit.

4.12. Any Customer hardware that is to be operated by a technician of the Provider as part of the Remote Hands additional service based on an agreement with the Provider must be designated by the Customer. If the Customer requests provision of the Remote Hands service, the Customer must properly and clearly identify the relevant hardware for the Provider; otherwise the service will not be provided.

4.13. The Customer must not make any audiovisual records on the Data Centre premises without the prior written consent of the Provider. If any audiovisual records are made, they must be made in the presence of a technician of the

Provider, unless otherwise agreed. The following objects must not be recorded under any circumstances: sensors, individual components of the automatic fire suppression system, laser systems, cameras and technologies of other customers or third parties. Any photographic documentation of the Customer's technology installed is permitted if made in the presence of a member of the Provider's staff.

4.14. The Customer must maintain confidentiality of all information concerning the Data Centre obtained by the Customer in any manner, especially information concerning the organisational, technical, safety and security measures concerning the Data Centre.

4.15. If the electricity power input into the Customer's space (rack, cage) is higher than the standard power consumption limit stipulated in the valid Service Description or the limit agreed in the Customer's Order or elsewhere in the Agreement, the Provider may send notice to the Customer that this limit has been exceeded and may ask the Customer to reduce the power input into the Customer's space (rack, cage) so as to comply with the standard power consumption limit provided for in the valid Service Description or the limit agreed in the Customer's Order or elsewhere in the Agreement within a reasonable deadline that must not be shorter than 48 hours. If the Customer does not ensure, by the given deadline, reduction of the power input into the Customer's space (rack, cage) based on the above request of the Provider, the Provider may take the steps specified in paragraph 5.4 of the Rules of Operation. If the Customer does not provably ensure and prove to the Provider within 5 business days from the suspension of the service that the power input into the Customer's space (rack, cage) is lower than or equal to the stipulated standard power consumption limit pursuant to the valid Service Description or any other limit agreed in the Customer's Order or elsewhere in the Agreement, the Provider may terminate the Agreement and/or the Customer's relevant Order based on a written notice of termination with immediate effect as of the date of delivery of such notice of termination to the Customer.

4.16. Each time when taking over a Data Centre service based on a protocol, the Provider will make the Customer acquainted with the following obligations and rules. The Customer undertakes to make any persons to whom the Customer allows entry to the technological space of the Data Centre acquainted with these obligations and rules in advance. These rules and obligations are as follows:

- arriving at and entering the Data Centre;
- opening and closing the front and rear doors of the rack;
- assembling and disassembling hardware;
- using the Provider's shared resources (consoles, steps, ladders);
- prohibition on installing Wi-Fi, GSM gates and similar transmitters without the prior express consent of the Provider;
- prohibition on installing any cables, equipment, objects and similar materials outside the leased space;
- prohibition on smoking, entering the technological space of the Data Centre under the influence of alcohol or drugs, bringing in and consuming drinks and food in this area;
- procedures for activating and using the automatic fire suppression system, including the location of the control and indication features;
- advice on the obligation to maintain confidentiality of all information concerning the Data Centre, especially the organisational, technical, safety and security measures concerning the Data Centre;
- first aid in the case of an electrical injury;
- advice on procedures in the event of loss or theft of the electronic chip card, visitor card or the key, including advice on the obligation to pay the contractual penalty in case of their loss.

4.17. The Customer will respect the following rules for equipment installation:

4.17.1. The Customer will install his/her equipment with regard to the generally recognised standards and in accordance with the applicable technical and legal regulations, the Agreement and other contractual documents, especially with these Rules of Operation, the Service Description or the Customer Order Form as well as with the Provider's instructions. In particular, the Customer will ensure proper air flow and compliance with the direction of equipment installation, namely the cold aisle – hot aisle if present or defined by the Provider upon takeover.

4.17.2. The Customer must ensure in the leased space that any open space in a rack in the direction of the cooling air flow is always blocked off. The Parties acknowledge that the cooling of air and air flow in the rack is a decisive parameter that may be influenced by changes in the infrastructure and position of the Customer equipment and/or cabling in the rack. For this reason, the Customer must optimise the position of his/her equipment and/or cabling in the rack, taking into account the air flow and cooling, the location of perforated tiles and the air flow in the vicinity of the rack, in accordance with the Provider's instructions.

4.17.3. In server rooms with contained cold aisles, it must be ensured that these aisles are permanently closed off. The design of the technologies in the Customer's rack must enable unused rack positions to be blocked off

as far as possible so as to keep minimum air overpressure in the cold aisle. This is the only way to achieve optimum cooling of all technologies installed.

4.17.4. In justified cases, the Provider will block off unused positions on the basis of paragraph 4.17.2., unless the Customer does so himself/herself to a sufficient degree. In the case of work of a large extent, such work will be consulted with the Customer in advance. The Provider's costs incurred by the blocking-off of the unused positions if made by the Provider will be invoiced to the Customer on a one-off basis, and the Customer is obliged to pay these costs to the Provider.

4.17.5. If necessary, the method of installation of particular equipment can be consulted with the Provider's staff or with the Help Desk staff at any time.

4.17.6. The Customer must not open windows in the administrative area of the Data Centre.

4.17.7. The Customer undertakes to comply with all conditions stipulated by these Rules of Operation (including any annexes thereto), the Service Description and/or the Agreement or the applicable legal regulations and technical standards. At the same time, the Customer must comply with the instructions of the Provider and the Provider's employees or with the instructions of the Provider's suppliers or such suppliers' employees in charge of the operation of the Data Centre.

4.17.8. The Customer is fully liable for the performance of the obligations by all persons to whom the Customer allows entry to the Data Centre, especially by the persons authorised to enter the Data Centre as designated by the Customer.

5. Rights and Obligations of the Provider

5.1. The Provider will allow the Customer access to the premises with the Customer's technology 24 hours a day.

5.2. The Provider does not bear any liability for the Customer's installed hardware and/or any equipment or any other item of the Customer located or brought in the Data Centre, unless the damage to such hardware was caused by the Provider breaching its obligations.

5.3. Where the Customer is suspected of being under the influence of alcohol or any other addictive substance, the Provider, or the Provider's competent authorised persons, including, in particular, Data Centre security staff, may prevent the Customer from entering the Data Centre or order the Customer to leave the Data Centre at any time. The above right to prevent the Customer from entering the Data Centre or to order the Customer to leave the Data Centre also applies if the Customer fails to comply with the instructions of the Provider or the Provider's authorised persons and/or with the conditions of these Rules of Operation or any other contractual documents, or with the applicable legal regulations.

5.4. If it is ascertained that the Customer's technology is installed in conflict with the conditions of the Rules of Operation and/or the conditions of the Agreement and/or the legal regulations in force and/or that the Customer breaches any other conditions stipulated by the Rules of Operation (or any annexes thereto) and/or the conditions of the Agreement or the legal regulations in force, the Provider may ensure that such technology is disconnected or put out of operation, or that the provision of the service is suspended, after the expiry of a reasonable deadline (of at least 48 hours) to no effect as stipulated by the Provider for the Customer to remedy the situation in a written notice of the breach of the conditions of the Rules of Operation and/or the Agreement or the breach of the legal regulations in force. If there is an imminent threat of damage, it is possible to disconnect the technology or put it out of operation, or suspend the provision of the service, even without notifying and informing the Customer in advance. If the Provider is forced to disconnect the Customer's technology or put it out of operation or suspend the provision of the service for the reasons specified here, the Provider will not be liable for any damage incurred by the Customer or third parties as a result thereof; in particular, the Customer will not be liable for any damage caused to the Customer's installed hardware and software, loss of data or any damage (including loss of profit) resulting from the fact that the service has been suspended or the Customer's technology has been disconnected or put out of operation.

5.5. If the Customer (or the persons authorised to enter the Data Centre or any other persons for which the Customer is liable, such as a supplier of the Customer) repeatedly breaches (breach) the conditions stipulated by the Rules of Operation (including any annexes thereto) and/or the Agreement or the legal regulations in force, the Provider may restrict the Customer's access to the Data Centre premises or directly terminate the Customer's Order and/or the Agreement by written notice with immediate effect as of the date of delivery of such notice of termination to the Customer.

6. Parking and Movement of Goods and Materials in the Data Centre

6.1. The parking places in the car park in front of the building are reserved for parking during the visit to the Data Centre.

6.2. When loading or unloading HW, the loading dock and loading platform may be used, with the assistance of an employee of the Provider, after notifying reception staff.

6.3. The Customer has access to the unpacking area/customer preparation area located at DC7 24x7. The customer preparation area is allocated for the prepping (configuration) of Customer hardware or software and for minor assembly work. Upon the completion of work, the Customer must immediately clear all remnants of materials (including packaging), exiting the workplace clean and orderly for the next customers to use as soon as possible.

6.4. Any storage of materials, hardware, equipment or any other items in the customer preparation area is prohibited. No Customer items must be left in the customer preparation area, i.e. the Customer must take all items with him/her when exiting. The Provider does not bear any liability for any hardware, materials, equipment or any other items located (left) by the Customer in the customer preparation area.

6.5. Where expressly agreed between the Customer and the Provider, the Provider will accept all consignments for delivery to the Customer, following prior notice, where the storage of such consignment is possible. The handover point will be a clearly designated unloading area inside the loading dock. The Provider will not be responsible for unloading the material from the vehicle or for any other required handling of the material. Furthermore, the Provider will never be liable for the condition and completeness of consignments unless stipulated otherwise by mutual written agreement. Unannounced consignments will not be accepted. Furthermore, the Customer will have 7 days in which to take over the consignment in person and on the premises and must process the consignment and dispose of packaging unless expressly agreed otherwise.

7. Safety and Automatic Fire Suppression System

7.1. A Customer entering the technological space of the Data Centre must comply with the safety regulations in force in the Czech Republic which apply to work on these premises. This means, in particular, Decree No. 50/1978 Coll., on professional competence in electrical engineering, as amended, and regulations concerning fire safety and occupational safety.

7.2. The Data Centre operates a strict prohibition on working with and handling naked fires and combustibles on its premises; a no-smoking policy is also in operation. All activities from which smoke or other fumes are produced, which could activate smoke/flame detection systems, are also prohibited.

7.3. Emergency exit – in the case of acute danger, the Customer may leave the area using the emergency exit. The Customer must immediately inform the Help Desk of the use of the emergency exit and must stay on the spot, outside the area with acute danger, until the arrival of the Provider's technician or the person in charge of safety.

7.4. Automatic fire suppression – the technological space is equipped with a self-extinguishing system that will be automatically activated in the case fire is detected. The following extinguishing agent is used:

7.4.1. The FM-200 gas, HFC 227ea, is a haloalkane – 1,1,1,2,3,3,3-Heptafluoropropane (CF3CHFCF3). In normal state, it is a colourless, odourless and electrically non-conductive gas. As an extinguishing agent, it is stored in liquid state under the pressure of 25 bar. When discharged, it changes to gaseous state in the nozzle. In the proper concentration, FM-200 extinguishes the fire by disrupting the combustion reaction. FM-200 quickly suppresses flames, prevents re-ignition, does not leave any residue and does not require clean-up after discharge – ventilation is required only. The system is designed to issue a quick response – within 10 seconds or less – so as to minimise damage to equipment and reduce the risk of loss of life. The amount of FM-200 required has been calculated in such a manner as to meet the strict requirements of the Factory Mutual Research Corporation (FMRC) and the National Fire Protection Association (NFPA). For areas where people are present, a safe concentration of the extinguishing agent has been designed pursuant to ISO 14520 as follows: 7.5% as the minimum and 9% as the maximum.

7.4.2. Inergen is a mixture of three gases (chemical substances) with inert properties and is composed of nitrogen (52%), argon (40%) and carbon dioxide (8%). Its composition does not harm the environment, it works based on the principle of the physical mechanism of extinguishment and has a stifling effect on the fire. The extinguishing effect of inert gases is achieved through the reduction of atmospheric oxygen below the limit value necessary for combustion (approx. below 13%). For this reason, it is absolutely necessary to ensure a safe evacuation of people in the shortest time possible, since, although breathing is possible in such an atmosphere, it may become difficult and, due to the toxic fumes from burning, even dangerous.

7.5. If the system detects a fire, this will be alerted by an acoustic alarm and a signal light.

7.6. If alarm is sounded, the Customer must immediately stop all activities and exit the area immediately. If gas nozzles are open, staying in this area poses a threat to life! The Customer must close the door behind him/her when exiting.

7.7. Once the system has been activated, the Customer is strictly prohibited from entering the area or opening the door repeatedly.

7.8. When the system is activated (acoustic alarm – siren, display panel), the Customer must contact the Help Desk upon exiting the area.

7.9. The Customer must not tamper with components of the fire detection and automatic fire suppression system in any way; especially manual activation of the system directly on the pressurized cylinders is prohibited.

7.10. The Customer may only activate the system manually using the yellow button in the case of a visual contact with the flame in the technological space of the Data Centre and if it is clear and obvious from the extent of the fire that the fire cannot be extinguished using a manual fire extinguisher.

7.11. All damage caused by the improper or unjustified activation of the system will be charged to the Customer in full; this includes payment of system contents, restoring the system and other damage caused by extinguishment.

7.12. Basic first aid information in case of exposure to gas:

- Eyes – rinse with water and call a physician;

- Skin – rinse with water; call a physician in the event of frostbite;
- Inhalation – move the person affected to fresh air and call a physician.

8. Personal Data Protection and Other Information

8.1. As the data controller pursuant to Article 4 of Regulation (EU) 2016/679 (the General Data Protection Regulation), the Provider will process the following data concerning the Customer and/or the persons authorised to enter the Data Centre for the purposes of their access to the Data Centre, including the issuance of access cards, checks on their authorisation to move around the Data Centre and the safeguarding of the legally protected interests of the Provider or third parties:

8.1.1. name, surname, identity document number, identification data of the Customer/supplier/any other entity, e-mail address and telephone number, mathematical representation of the biometric template, information on accesses, and PIN, if assigned

8.1.2. and will do so for the period strictly necessary but, at a maximum, (a) for a period of 2 months from the date the Access Permission was cancelled for any reason if the processing takes place on the grounds of the performance of the Agreement/Customer Order Form (allowing entry to the Data Centre premises and the provision of the Data Centre services), (b) for a period of 12 months from the date on which the person authorised to enter the Data Centre ceases to be a person authorised to enter the Data Centre if the processing takes place on the grounds of the legitimate interests of the Provider (controller) or third parties (ensuring the security of the Data Centre, raising of any legal or other claims), with the exceptions specified below, or if stipulated by the legal regulations in force.

8.2. A CCTV and access system operated by the Provider or a person authorised to do so by the Provider has been installed in the Data Centre.

8.3. The CCTV records are stored for a period of 30 days.

8.4. The access system performs

8.4.1. monitoring of the legitimacy of access to the premises and/or movement within the premises;

8.4.2. comparison of the sample (mathematical representation of the biometric template) stored in the system/on the access card with the sample obtained in real time by the person authorised to enter the Data Centre placing his/her finger on the system reader. For the sake of completeness, it is stated that the system used by the Provider does not process biometric templates (fingerprints), i.e. the image or scan on which the biometric template is recorded. When a person places his/her finger on the reader, the system is able to use certain one-way mathematical functions to generate a number sample from the biometric template, which is subsequently recorded in the system. Any intended use of the number sample in any other system would not be possible, as the sample could not be processed by any other system. Any biometric template initially provided by a person authorised to enter the Data Centre for the purpose of entering selected areas becomes generally unreadable and cannot be restored by the system.

8.5. Each person in relation to whom the Provider processes personal data has the right to access to the personal data, the right to rectification, explanation, removal of a state occurred, especially to the rectification, supplementation or destruction of his/her data; such person may contact the Personal Data Protection Office. Data subjects may exercise their rights using the contact details listed in these Rules of Operation.

8.6. The processor/recipient of the data is

8.6.1. CE Colo,

8.6.2. Sitel,

8.6.3. Wakkenhat Zeta.

9. Validity and Effect of the Rules of Operation

9.1. The Rules of Operation are valid and effective from 1 June 2018.

9.2. The Provider reserves the right to unilaterally amend the Rules of Operation at any time in connection with any changes in the products and services or in connection with any other circumstances concerning the operation of the Data Centre and/or the provision of the Data Centre services. The Provider is obliged to inform the Customer of any such changes in advance.

10. Annexes

- Fire Evacuation Plan
- Fire Alarm Policy
- Help Desk
- Authorised Persons List (Form)

- Access Rules
- Advice