



# beyond.pl

FIRMA BEYOND.PL SP. Z O. O.

ul. Adama Kręglewskiego 11

61-248 Poznań

## **IDW-04 - DATA CENTER 1 POLICY**

Document indication:	IDW-04
Version:	04
Date of issue:	2019-08-09
Created by:	Grzegorz Schilf, Dariusz Sobkowiak
Approved by:	Board
Confidentiality level:	Internal Unclassified

**CHANGELOG**

<b>Date</b>	<b>Version</b>	<b>Created by</b>	<b>Change description</b>
2019-03-12	02	Dariusz Sobkowiak	Change of title, minor modifications in content.
2019-08-05	03	Dariusz Sobkowiak	Point 4.4 related to the principles of personal data processing added.
2019-08-09	04	Aleksandra Urbanowicz	Implementing Personal Data Processing Information Clause.

## Contents

<b>1. GOAL OF THE PROCEDURE, RANGE, USERS .....</b>	<b>4</b>
<b>2. DEFINITIONS .....</b>	<b>4</b>
<b>3. DESCRIPTION OF THE DATA CENTER 1 .....</b>	<b>5</b>
3.1. Location and Equipment .....	5
3.2. Zone Description .....	5
3.2.1. General Information .....	5
3.2.2. Security Zones .....	5
3.3. Data Center 1 Management.....	7
3.3.1. Personnel Structure.....	7
3.3.2. Services Management Center .....	7
3.4. Communication Policy.....	7
3.4.1. Important Contacts .....	7
3.4.2. Customers.....	8
3.4.3. Maintenance .....	8
3.4.4. Couriers and Postal Deliverers .....	8
<b>4. ADDITIONAL INFORMATION.....</b>	<b>8</b>
4.1. Standing Orders.....	8
4.2. Information Security.....	9
4.3. Penalties for the Breach of Data Center 1 Policy .....	10
4.4. Personal Data Protection .....	10
<b>5. RELATED DOCUMENTS .....</b>	<b>11</b>

## 1. Goal of the Procedure, Range, Users

This document contains the information about the location of the Data Center 1 Beyond.pl, its infrastructure, security system configuration, operational structure, and service rules.

All information contained herein is confidential. No part of this document can be copied or used for purposes other than those for which it has been supplied without prior written consent of Beyond.pl.

This document applies to all Beyond.pl employees and contractors (including agents, subcontractors, business units, natural persons, and legal entities), depending on their tasks performed for the benefit or on behalf of Beyond.pl.

## 2. Definitions

For the purposes of this policy, the following terms and definitions apply:

**Data Centre 1 (the Facility)** - a complex of technology rooms including server chambers, the necessary technical facilities (i.e. uninterruptible power supply systems, cooling systems), the Data Centre 1 Service Management Centre, and social and living quarters;

**Administrator** – Beyond.pl Sp. z o.o., registered in Poznań, ul. Adama Kręglewskiego 11, entered in the Register of Entrepreneurs of the National Court Register under KRS 0000237620;

**ZOT** - Zespół Obsługi Technicznej (Technical Service Team) at Data Center 1;

**Service** - entity providing supplies, performing finishing works, repairs, or maintenance at the Facility;

**Guest** - person present at the Facility and invited by the Administrator's employee;

**Klient** - podmiot korzystający z usług Data Center 1 na zasadach i w zakresie określonym przez Umowę;

**Customer** - entity using Data Center 1 services to the extent determined by the Agreement;

**Agreement** - agreement between the Administrator and the Customer, defining specific terms of reference for the services provided;

**Colocation Space** - Cage, Server Rack, rack space, or any other combination and number of the above specified in the Order;

**Infrastructure** - Administrator's equipment and accessories used to perform Services;

### 3. Description of the Data Center 1

Rozdział zawiera opis Obiektu Data Center 1. This chapter provides a description of the Data Center 1.

#### 3.1. Location and Equipment

Data Centre 1 Beyond.pl is located in the Old Brewery building in Poznan, within the boundaries defined by Półwiejska Street to the south-east, Kościuszki Street to the south-west and Gen. J. H. Dąbrowskiego Park to the north-east. For the Data Centre 1

in the Old Brewery building, a number of changes were made to increase the security of the Facility. Traffic and pedestrian routes were modified. Cable runs were doubled. Elements posing a potential hazard (ducts, water pipes) were removed. A secure unloading ramp was located in the immediate vicinity.

#### 3.2. Zone Description

##### 3.2.1. General Information

Data Centre 1 architecture takes into account customers' needs for simplicity of access to their own space together with full physical security.

Data Centre 1 - Entrances:

- personnel entrance (main entrance),
- technical entrance (from the unloading ramp) equipped with a lift to enable deliveries to be made.

Both entrances are equipped with passageway locks to increase the security of the Facility. There is a perimeter corridor running around the colocation space allowing for the separation of Clients (dedicated entrance for the Client to their colocation space).

A welfare and living area has been prepared for the Users of Data Centre 1.

##### 3.2.2. Security Zones

Due to security reasons, the facility and its immediate surroundings have been divided into different security zones depending of the level of risk and rights of access. The facility is protected on 24-hour basis by Security Guards of Old Brewery.

Each entrance to Data Centre 1 requires the use of a videophone to report presence to staff.

###### 3.2.2.1. Outdoor Area

Outdoor area includes: all outdoor areas adjacent to Data Center 1. Access to the area is not restricted but is covered by the Old Brewery Security CCTV. The area is regularly patrolled by the Security personnel.

### 3.2.2.2. Hospitality Area

The hospitality area includes: the social room area, the hospitality mezzanine, and the corridor connecting these rooms. Access to the zone from the outside is monitored by an intercom system. Being in this zone does not require the activation of an access card, but the entry itself must take place in the presence of an authorised representative: Administrator or Customer. It is the responsibility of the person entering to instruct the Guest about the rules in force on the premises and to report the Guest's presence on the premises to the resort staff. Such a person shall be registered in the F-44 - Visitor's Entry Log Book and shall sign a declaration that he/she has read the Rules and Regulations of Data Center 1 Beyond.pl, the specimen of which is a form F-65 of these Policy.

### 3.2.2.3. Service Access Zone

Service access zone covers room(s) with access route for deliveries, repairs, or maintenance. Access to the service zone requires prior notification by e-mail to [prace.dc1@beyond.pl](mailto:prace.dc1@beyond.pl).

Maintenance work may be performed only in the presence of a ZOT employee or an authorised Beyond.pl representative.

### 3.2.2.4. Loading/Unloading Area

Loading/unloading area is part of the Service Access Zone. The area can be accessed subject to prior notification according to section 8 of the IDW-06 Infrastructure Service Policy Beyond.pl.

Access to the loading/unloading area does not require the activation of a service card. Unloading may only take place in the presence of a ZOT employee or an authorised Beyond.pl representative.

Access to the loading/unloading zone is preceded by a check at the Old Brewery security post. After positive verification, security allows access to the loading/unloading zone.

A detailed procedure regulates the handling of receipts and deliveries:

**P-33 - Collection and Supply Handling (Delivery Zone) - Customers and Maintenance Services.**

**P-34 - Collection and Supply Handling (Delivery Zone) – DC1 Personnel.**

### 3.2.2.5. Customer Access Zone

The Customer zone includes: the guest zone, perimeter corridors and the collocation space specified in the contract/order. Staying in this area requires the activation of a user access card - issued at the request of a user with an active contract. Cards are issued to authorised persons on behalf of the Customer, as indicated in the relevant appendix to the Agreement. The Customer's access card does not have to be returned upon completion of the work and can be used 24 hours a day without restriction. The user's entry to the facility does not need to be agreed with the staff - with the exception of visitor entry. An access card and proof of identity are required on the Data Centre premises. The card or document must be presented whenever requested by the staff of the Data Center 1. The staff must be immediately notified of the loss of the access card.

Detailed rules applicable to the Customer's access area are set out in **IDW-06 - Infrastructure Terms of Service**.

#### **3.2.2.6. Employee Access Zone**

Employee Access Zone covers all rooms, including Customer Zone inside the Data Center 1. Employees move around the facility using access cards. Employee Access Zone is divided into different access levels, which are assigned in accordance with the principle of necessity.

Access to the Customer's Zone using the employee's card shall only take place in reasonable cases, and records of entry shall be available to the Customer upon request.

The detailed rules for activating cards and assigning access levels to an employee are governed by procedure **IDW-30 – Instruction on Handling Physical Access Control Cards**.

### **3.3. Data Center 1 Management**

#### **3.3.1. Personnel Structure**

The performance of Data Center 1 services is supervised by the Data Center Management Team. The team members have passed the company verification and training process. Data Center Management Team is divided into the Technical Service Team (ZOT) and the IT team supervising IT systems and providing support services for the Data Center 1 customers.

#### **3.3.2. Services Management Center**

The ZOT technical team and the IT services team are stationed at the DC Services Management Center. It is a room located on the first floor of Data Centre 1, equipped with a complete service monitoring system, alarm notification system, and a remote infrastructure management and diagnostics system.

### **3.4. Communication Policy**

#### **3.4.1. Important Contacts**

- **Helpdesk**  
Tel. +48 616674800  
help.desk@beyond.pl
- **Technical Service Team (ZOT)**  
Tel. kom. 667 624 220  
prace.dc1@beyond.pl
- **Old Brewery Security**  
Tel. kom. 604 958 100

### 3.4.2. Customers

Detailed rules for communication, notification of deliveries and visits for Customers using colocation services are defined in **IDW-06 - Infrastructure Terms of Service**.

Detailed communication rules for Customers using other services are defined in each case in the Agreement.

### 3.4.3. Maintenance

Maintenance companies are required to submit a completed **F-38 Application of Permission to Perform Works** by 15:00 of the preceding day to [prace.dc1@beyond.pl](mailto:prace.dc1@beyond.pl).

The handling of the maintenance visit is detailed in the procedure:

**P-45 - Application of Permission to Perform Works Handling Procedure – DC1 Personnel.**

**P-46 - Application of Permission to Perform Works Handling Procedure - Maintenance Services.**

### 3.4.4. Couriers and Postal Deliverers

Data Center 1 personnel are required to follow procedure **P-27 - Courier and Postal Delivery Handling Procedure Data Center 1**.

## 4. Additional Information

### 4.1. Standing Orders

- Persons authorised by the Client are obliged to carry on the premises of Data Centre 1 badges or access cards issued by the Administrator in accordance with the applicable security procedure, and to show proof of identity at the request of centre staff.
- While at the facility, it is strictly forbidden to:
  - being under the influence of alcohol,
  - **bring any pyrotechnic devices, explosives, or weapons, including firearms, blade weapons, teasers, stun guns, tear gas, or similar tools (does not apply to uniformed services),**
  - consume alcohol or smoke outside designated areas, or bring and use drugs, or psychotropic substances,
  - record videos or take pictures without permission from the facility management,
  - leave baggage or any other objects which may interfere with the operation of the facility unattended,
  - litter or pollute facility area,
  - use open fire or spray fragrances and smoke,
  - park vehicles outside designated areas.
- Transport of hazardous substances, particularly infectious agents, explosives, or radioactive materials is strictly prohibited.
- Transport of potentially hazardous substances, including acids, pyrophoric materials, compressed gas, flammable materials, combustible materials, poisonous substances, cooling agents, toxic substances, or volatile substances, is only permitted in justified



cases. Visitors shall justify the above transports in the form **F-38 - Application of Permission to Perform Works - Maintenance Services**. Customers are forbidden to transport any hazardous materials.

- It is forbidden to arrive at the Data Center 1 with visitors who have not been granted access permission by a member of staff.
- Everyone who encounters a person without an ID, is obliged to notify the Data Center 1 personnel.
- Data Center personnel can request a person without a visitor badge or an ID, or not complying with the Data Center Policy or the facility security procedures, to leave the premises.
- When you lose your access cards, you should report it to the Security or a ZOT employee on duty.
- It is forbidden to bring any liquids into electrical or technical rooms, including server rooms.
- In case you hear fire alarm, you must immediately go towards emergency exits and strictly adhere to ZOT and Security instructions.
- In the event of damage to the Data Centre 1 facility that is not the result of from normal operation, caused by the fault of the persons representing the Customer, the Customer shall be obliged to cover the actual costs. In particular, this applies to cases of:
  - destruction or damage of the facility or facility equipment,
  - damage of hardware components or disruption of Service resulting from unauthorised configuration changes or repairs by Customer employees,
  - causing fire, floods, etc.,
  - causing false alarms or unjustified use of security services,
  - degrading Administrator provided services by unjustified and unauthorised involvement of facility staff,
  - disturbing air conditioning process by leaving equipment or packaging outside designated areas.

## 4.2. Information Security

**All persons who visit Data Center 1 are obliged to keep confidential all information they have received while at the premises. This applies in particular to the technical, process, legal, and organisational information regarding ITC systems and networks, as well as data contained therein.**

Confidential information is company secret within the meaning of the Unfair Competition Act of 16 April 1993 (i.e. Journal of Laws 2003, No 153, item 1503, as amended) disclosed verbally, in writing, or otherwise.

The above shall not apply to the disclosure of information:

- publicly available;
- obtained independently from other legitimate sources;
- with written permission to distribute,
- required by law.

The above shall apply to taking photos of the Data Center 1, particularly the equipment and server room location. Photography of the above without written consent from the Beyond.pl Board is strictly prohibited. Photo documentation of the Customer's infrastructure is possible upon prior arrangements. The Customer is required to submit written request with details of the documentation. Upon obtaining an approval, the Customer can take photos of their own infrastructure and under staff supervision only and under the condition, that copy of the photos are handed over to the Data Center Administrator.

All persons who visit Data Center 1 are obliged to adhere to policy rules, procedures and information security instructions applicable at the premises.

All persons who obtain confidential information are prohibited from:

- copying and disclosing such information to unauthorised persons,
- transferring such information to third parties by any means,
- making profit with information obtained,
- offering the sale of confidential information.

Persons who obtain information shall return all documentation, materials, and storage media they come into possession as part of services performed for the benefit of the Administrator.

The obligation of professional secrecy regardless of the information form shall apply for the period of 5 (five) years, starting from the date a visit to the Facility has finished.

Beyond.pl has the right to pursue their claims in court in the event of breach by of the provisions of Art. 4.2.

### 4.3. Penalties for the Breach of Data Center 1 Policy

Administrator has the right to apply the following penalties against persons, who do not adhere to Data Center 1 Policy:

- Warning,
- Warning with notification to dedicated Customer representative,
- Removing authorized person from the premises and deactivating their access card.

Beyond.pl shall claim compensation from the Guest or the Customer who was in breach of this Data Center 1 Policy causing damage.

### 4.4. Personal Data Protection

Personal Data Controller is Beyond.pl Sp. z o.o., with registered office at ul. Adama Kręglewskiego 11, 61-248 Poznań, Poland. Beyond.pl Sp. z o.o. appointed a Personal Data Protection Supervisor, whom you can contact by sending an email to [iod@beyond.pl](mailto:iod@beyond.pl). Data is collected to process your visit at Data Center 2, and to ensure property protection and security at Controller's premises. Providing personal data is voluntary, however, refusal to provide personal data will make visits to our facilities impossible. Your data is processed under RODO art. 6(1)(f), i.e. Controller's legitimate interest in verifying your identity due to the security

screening standards adopted by the certifying authorities (ANSI - TIER IV; TUV SUD - ISO 27001: 2013) and the PCI DSS standard compliance requirements. The extent, to which you and Beyond.pl Sp. z o.o. are contractually bound or your visit at Beyond.pl Sp. z o.o. premises for the purpose of negotiating or concluding an agreement, the basis for personal data processing are the concluded agreement or actions leading to its conclusion in the future (RODO art. 6(1)(b)). The scope of the data processed by Beyond.pl Sp. z o.o. corresponds to the scope of the data indicated in the relevant procedure, statement, application or regulations applicable to a particular visit at Data Center 2, listed under section 5 - "Related Documents" of this instruction. The scope of data also includes recorded video surveillance image

The company Beyond.pl Sp. z o.o. processes the data in a manner consistent with the current legal provisions, only for the purpose of fulfilling your visit and ensuring the security of the facility. Your data will be processed for a period of 36 months. Your recorded video surveillance image data will be processed for a period of 3 months. You have the right to access, copy, amend, rectify, delete, restrict data processing, transfer and object to the processing of your data. You also have the right to lodge a complaint with a supervisory authority if you consider that your data is not processed lawfully. Your data may be made available to the company providing security services and keeping entry and exit records at the Controller's facilities. Your data will not be transferred outside the European Economic Area. Beyond.pl does not profile your data, including automated decision making.

If you want to know more about your personal data send us an e-mail to: **help.desk@beyond.pl** or visit the following website: **<https://www.beyond.pl/en/personal-data-protection>**.

## 5. Related Documents

IDW-06 - Infrastructure Terms of Service;  
F-38 - Application of Permission to Perform Works;  
F-65 - Statement of Understanding;  
IDW-30 – Instruction on Handling Physical Access Control Cards; \*  
P-27 - Courier and Postal Delivery Handling Procedure Data Center 1; \*  
P-33 - Collection and Supply Handling (Delivery Zone) - Customers and Maintenance Services;  
P-34 - Collection and Supply Handling (Delivery Zone) – DC1 Personnel; \*  
P-45 - Application of Permission to Perform Works Handling Procedure - DC1 Personnel; \*  
P-46 - Application of Permission to Perform Works Handling Procedure - Maintenance Services.

- \* - **INTERNAL PROCEDURES - AVAILABLE FOR AUTHORIZED CBTI PERSONNEL ONLY.**

**Approved by**

**Board**