



**Independent Service Auditor's Assurance  
Report on the Description Data Centers  
Facilities of **Data4 Services** and the  
Suitability of the Design and Operating  
Effectiveness of Controls for the Period from  
November 1, 2023 through October 31, 2024**

**Type II report following ISAE 3402 standard**

## Table of Contents

I.	Independent Service Auditor's Assurance Report.....	1
II.	Management's Assertions.....	3
III.	Management's Description of Infrastructures and Controls.....	4
A.	Scope and Purpose of the Report.....	4
B.	Data4 Group presentation.....	5
C.	Infrastructure description on Marcoussis and Dual Building sites in France.....	7
D.	Data Center operations and environmental controls.....	13
IV.	Auditor's description of system and controls.....	16
V.	Other information provided by Data4 Services.....	25

## **I. Independent Service Auditor's Assurance Report**

To the Management of Data4 Services

### *Scope*

We have examined Data4 Services (the "Company") description of its Data Centers Facilities activities (the "Description" or "System") throughout the period from November 1, 2023 through October 31, 2024 ("Specified Period"), and the suitability of design and operating effectiveness of controls to achieve the related control objectives stated in the Description.

### *Data4 Services Responsibilities*

In Section III of this report, Data4 Services has provided an assertion about the fairness of the presentation of the Description and suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the Description.

Data4 Services is responsible for preparing the Description and for the accompanying assertion, including the completeness, accuracy, and method of presentation of the Description and the assertion, providing the services covered by the Description, specifying the control objectives and stating them in the Description, identifying the risks that threaten the achievement of the control objectives, selecting the criteria, and designing, implementing, and documenting controls to achieve the related control objectives stated in the Description.

### *Service Auditor's Responsibilities*

Our responsibility is to express an opinion on the fairness of the presentation of the Description and on the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the Description, based on our examination. We conducted our examination (assurance engagement) in accordance with the International Standard on Assurance Engagements 3402, "Assurance Reports on Controls at a Service Organization," issued by the International Auditing and Assurance Standards Board. Those standards require that we comply with ethical requirements and plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is fairly presented, and the controls were suitably designed and operating effectively to achieve the related control objectives stated in the Description throughout the Specified Period.

An examination of a description of a service organization's system and the suitability of the design and operating effectiveness of the service organization's controls to achieve the related control objectives stated in the description involves performing procedures to obtain evidence about the fairness of the presentation of the description and the suitability of the design and operating effectiveness of those controls to achieve the related control objectives stated in the description. Our procedures included assessing the risks that the Description is not fairly presented and that the controls were not suitably designed or operating effectively to achieve the related control objectives stated in the Description.

Our procedures also included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the related control objectives stated in the Description were achieved. An examination engagement of this type also includes evaluating the overall presentation of the Description and the suitability of the control objectives stated therein, and the suitability of the criteria specified by the Company and described in Section II and III of the report. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

### *Limitations of Controls at a Service Organization*

Data4 Services's Description is prepared to meet the common needs of a broad range of customers and their auditors and may not, therefore, include every aspect of the System that each individual customer may consider important in its own environment. Also, because of their nature, controls at the Company may not prevent, or detect and correct, all errors or omissions as part of its colocation services. Also, the projection to the future of any evaluation of the fairness of the presentation of the Description, or conclusions about the suitability of the design or operating effectiveness of the controls to achieve the related control objectives is subject to the risk that controls at Data4 Services may become inadequate or fail.

This report is intended solely for the information and use of Data4, customers of Data4 Hosting services, and the independent auditors of such customers.

**Data4 SERVICES – ISAE 3402 TYPE II REPORT**  
**SECTION I. INDEPENDENT SERVICE AUDITOR'S ASSURANCE REPORT**

---

*Subservice Organization*

The Company don't rely upon subservices organizations, located in Marcoussis, France, to host in its datacenter client infrastructures. The Description in Section III of this report includes only the controls and related control objectives of the Company and for the organization providing data centers's colocations services. Our examination did not extend to the controls of a subservice organization.

*Opinion*

In our opinion, in all material respects, based on the criteria described in Data4 Services's assertion in Section II of this report:

- (a) The Description fairly presents the Data Centers Facilities of Data4 Services that was designed and implemented throughout the specified period ;
- (b) The controls related to the control objectives stated in the Description were suitably designed to provide reasonable assurance that the control objectives would be achieved if the controls operated effectively throughout the Specified Period; and
- (c) The controls tested, which were those necessary to provide reasonable assurance that the control objectives stated in the description were achieved, operated effectively throughout the Specified Period (except from some identified exceptions, mentioned in section IV of this report).

*Description of Tests of Controls*

The specific controls tested, and the nature, timing and results of those tests are listed in Section IV of this report.

*Intended Users and Purpose*

This report, including the description of tests of controls and results thereof in Section IV of this report is intended solely for the information and use of Data4 Services, user entities ("customers") of Data4 Services's Data Centers Facilities during some or all of the Specified Period, and the independent auditors of such customers, who have a sufficient understanding to consider it, along with other information, including information about controls implemented and operated by customers themselves, when assessing the risks of material misstatements of customer's financial statements. The report is not intended to be and should not be used by anyone other than these specified parties.

Neuilly-sur-Seine, 5 december 2024

Alexis GRIN, Partner,

Cyril BROGNIART, Partner,

**For Grant Thornton France**  
**French Member Firm of Grant Thornton International**

This report is intended solely for the information and use of Data4, customers of Data4 Hosting services, and the independent auditors of such customers.

## **II. Management's Assertions**

The accompanying description has been prepared for clients who have used the Data4 Services's (the "Company") Data Centers Facilities and their auditors who have sufficient understanding to consider the description, along with other information, including information about controls operated by user entities ("clients") themselves, when obtaining an understanding of clients' information systems relevant to financial reporting. Data4 Services S.A. confirms that:

(a) The accompanying description in Section III fairly presents Data4 Services Data Centers Facilities and the related tests of operating effectiveness for the period from November 1, 2023 through October 31, 2024 ("Specified Period"). The criteria used in making this assertion were that the accompanying description:

(i) Presents how the system was designed and implemented, including:

- The types of services provided, including, as appropriate, classes of transactions processed.
- The procedures, within both information technology and manual systems by which those transactions are initiated, authorized, recorded, processed, corrected as necessary, and transferred to reports for the clients.
- How the system dealt with significant events and conditions, other than transactions.
- The process used to prepare reports for customers.
- Controls that we assumed, in the design of the system, would be implemented by user entities, and which, if necessary, to achieve control objectives stated in the accompanying description, are identified in the description along with the specific control objectives that cannot be achieved by Data4 Services alone.
- Other aspects of the Company's control environment, risk assessment process, information systems (including related business processes) and communication, control activities, and monitoring controls were relevant to the processing and reporting client transactions.

(ii) Does not omit or distort information relevant to the scope of Data Centers Facilities being described, while acknowledging that the description is prepared to meet the common needs of a broad range of clients of the services and their auditors, and may not, therefore, include every aspect of Data Centers Facilities that each individual client of the services and its auditor may consider important in its own particular environment.

(b) The controls related to the control objectives stated in the accompanying description were suitably designed and operated effectively throughout the Specified Period. The criteria we used in making this assertion were that:

(i) The risks that threatened achievement of the control objectives stated in the description were identified by Data4 Services ;

(ii) The identified controls would, if operating as described, provide reasonable assurance that those risks would not prevent the control objectives stated in the description from being achieved; and

(iii) The controls were consistently applied as designed, including whether manual controls were applied by individuals who have the appropriate competence and authority.

(c) Due to our confidentiality clause, prohibiting us from disclosing confidential and strategic corporate information, documentation of applied controls has not been transmitted to auditors for archiving and traceability purposes. It has been consulted in our offices on the Marcoussis site.

Marcoussis, 4 december 2024  
Jean-Paul Leglaive  
Head of QHSE, Data4 Services



This report is intended solely for the information and use of Data4, customers of Data4 Hosting services, and the independent auditors of such customers.

### **III. Management's Description of Infrastructures and Controls**

#### **A. Scope and Purpose of the Report**

This document describes Data4 Services. (the "Company") Data Centers Facilities provided to its customers by its Data Centers Facilities team throughout the period of November 1, 2023 through October 31, 2024 ("Specified Period") and assess the suitability the of design and operating effectiveness of controls to achieve the related controls objectives stated in the description.

The description of Data4 Services is limited to access control and security devices installed in the Data Centers Facilities to ensure that the client facilities are suitably exploited.

Data4 Services Management is responsible for the identification of the control objectives and for the manual and system-based control policies and procedures to achieve those objectives. This report is intended solely for the information and user of Data4 Services, user entities ("customers") of colocation services, and the independent auditors of such customers, who have a sufficient understanding to consider it, along with other information, including information about controls implemented and operated by customers themselves, when assessing the risks of material misstatements of customer's financial statements. The report is not intended to be and should not be used by anyone other than these specified parties.

Controls described in this report are applicable to Data Centers managed in France by Data4 Services for all its clients. The scope of this report includes 20 data center facilities in operation :

- 7 buildings "design X" (DC01 / 02 / 03 / 04 / 07 / 08 / Dual Building)
- 4 buildings "design Y" (DC05 / 06 / 09 / 10)
- 4 buildings "design Y'" (DC11 / 12 / 14 / 15 / 16 / 17 / 19)
- 1 buildings "design Y'" (DC18 / 20)

The report was prepared according to the guidance contained in the International Standard on Assurance Engagements ("ISAE") standard No. 3402, "Assurance Reports on Controls at a Service Organization", issued by the International Auditing and Assurance Standards Board.

## **B. Data4 Group presentation**

### **1 European data center operator**

Data4 Services is a European data center specialist which currently operates 36 data centers in Paris, Milan (Cornaredo), Madrid (Alcobendas), Warsaw and Luxembourg:

- 37 data centers built (+ 21 additional constructible buildings)
- 860 MW total power capacity
- 165 hectares total land capacity
- 169,47 MW Total IT Space capacity
- Certified Data Centers

### **2 European strategic sites**

The Data4 Services' sites have state of the art datacenters, Hyper-connected infrastructures and DRP in Paris – Dual site 7 km fibers away. They are in a secure location, without any environmental, social or transport risk. Close to the heart of Paris, Milan, Madrid & Luxembourg.

#### **Energy**

Since 2018, equivalent of 100% of consumption produced from Renewal Energy Sources.

#### **Compliance**

Data4 Services has implemented an Integrated System Management (ISM) at double level:

- Multi-ISO standards (9001, 14001, 27001, 45001, 50001) + HDS + PCIDSS + European Code of Conduct for Data Centers
- Multi-sites

To better cover customers' needs for quality of services, security, legal & regulatory compliance, environmental & energy performance. This approach is part of continuous improvement strategy of Data4 Services.

#### **ISO Certifications, HDS certification and PCIDSS certification**

The International Organization for Standardization (ISO) is the largest organization in the world for the creation and publication of international standards. The ISO certification signifies that Data4 Services can offer products and services which meet or exceed its clients' specifications, by implementing quality, safety, health, environmental protection and energy management standards, in their widest possible sense for the IT sector.

- ISO 9001: 2015 (Marcoussis, Dual Building, Cornaredo, Warsaw)  
Activity Certified: development and commercialization of secured IT hosting of IT infrastructure and maintenance in operational conditions of data center infrastructures  
Starting date of the certification: 18<sup>th</sup> February 2016  
End of the current cycle: 17<sup>th</sup> February 2022
- ISO 27001: 2013 (Marcoussis, Dual Building, Cornaredo, Alcobendas, Warsaw)  
Activity Certified: Information security management system for hosting of IT infrastructure  
Starting date of the certification: 03<sup>rd</sup> February 2016  
End of the current cycle: 02<sup>nd</sup> February 2025
- ISO 45001: 2018 (Marcoussis, Dual Building, Cornaredo, Alcobendas)  
Activity certified: development and commercialization of secured IT hosting of IT infrastructure and maintenance in operational conditions of data center infrastructures  
Starting of the certification: 07<sup>th</sup> March 2019  
End of the current cycle: 06<sup>th</sup> March 2022

This report is intended solely for the information and use of Data4, customers of Data4 Hosting services, and the independent auditors of such customers.

- ISO 14001: 2015 (Marcoussis, Dual Building, Cornaredo, Alcobendas)  
Activity certified: development and commercialization of secured IT hosting of IT infrastructure and maintenance in operational conditions of data center infrastructures  
Starting date of the certification: 18<sup>th</sup> February 2016  
End of the current cycle: 17<sup>th</sup> February 2022
- ISO 50001: 2018 (Marcoussis, Dual Building, Cornaredo, Alcobendas)  
Activity certified: développement et commercialization de solutions d'hébergement informatique sécurisé et maintien en condition opérationnelle des infrastructures data center  
Starting of the certification: 09<sup>th</sup> March 2019  
End of the current cycle: 09<sup>th</sup> March 2022
- HDS: v1.1 juin 2018 (Marcoussis, Dual Building)  
Activity certified: mise à disposition et maintien en conditions opérationnelles du site physique permettant d'héberger l'infrastructure matérielle du système d'information utilisé pour le traitement des données de santé – mise à disposition et maintien en condition opérationnelle de l'infrastructure matérielle du système d'information utilisé pour le traitement des données de santé  
Starting of the certification: 28<sup>th</sup> April 2023  
End of the current cycle: 27<sup>th</sup> April 2026
- PCIDSS: v4.0(France only – DC01 / DC02 / 03 / 04 / 05 / 06 / 08 / 10 / 11 / 14 / 15 / 16 / 18 / 20 / Dual Building)  
Activity certified: physical space (co-location) – physical security  
Duration of certificate: 17<sup>th</sup> April 2024 – 17<sup>th</sup> April 2025
- European Code of Conduct for Data Centers (France: DC01 to DC14 / Dual Building – Italy: DC01 to DC03 – Spain: DC01 – Luxembourg: DC01)  
Economic and energy supply security impacts  
Renewal: 2021

### **Risk assessment**

As part of its integrated management system, Data4 Services has implemented a Business Risks assessment initiative beginning of 2016. Through workshops with Data4 Services management following a Top-Down approach, Data4 Services has identified its business risks leading to consider major risks (internal and external). These risks have been quoted and for each one an associated action plan has been developed for managing the security information risks but also the environmental, energy, health and safety risks (pollution, flood, earthquake, social movement, forest fire, physical safety problem, monitoring unavailability, weather unavailability, network failure etc.).

The management system of Data4 Services is in line with the requirements for the **development and commercialization of secured IT hosting of IT infrastructure and maintenance in operational conditions of data center infrastructures**.



## **C. Infrastructure description on Marcoussis and Dual Building sites in France**

The site of Marcoussis (including the Dual Building) is the largest and most powerful data center campus in Europe. The site is based in the dynamic cluster of Paris Saclay on Net IT Space: 21300 sqm. There are 20 data centers in operation with power capacity of 100 MW, 7 buildings “design X”, 4 buildings “design Y”, 7 buildings “design Y” and 2 building “design Y”.

### **Site access Buildings**

Marcoussis site is divided in 3 different areas before access to computer rooms:

- 1. Campus zone**
  - Security check: Limited access by badge (permanent or temporary)
  - Safety grid around the zone's perimeter.
  - CCTV controls
  - Access by unipersonal airlock (human or vehicle)
- 2. DC zone**
  - Security check: Limited access by badge (permanent or temporary)
  - CCTV controls
  - The perimeter of the zone is also protected (grid / anti-crossing system - electronics)
- 3. DC building within DC zone**
  - Limited access by unipersonal airlock and badge, at each DC building.
  - Badge control system to access shared spaces and computer rooms.
  - The technical rooms in the data centers are accessible with keys managed and controlled by a secure electronic safe (with a password login).

All data centers are divided into several blocks with dedicated spaces and shared spaces according to the contractual relationship defined with the customer. Biometric systems are used at the request of customers.

### **Prevention/detection device**

- Fire detection and HSSD (High Sensitivity Smoke Detection facilities)
- Humidity sensors - ambiance (atmospheric)
- Temperature sensors Atmos and returned air
- Public spaces are covered by CCTV, and for private spaces (customers) is on demand.

### **Air conditioning/cooling systems**

Air conditioning facilities have N+1 or N+2 level of redundancy. The air conditioning devices and infrastructures are located outside the servers/customers' rooms - but inside the building, in the technical corridors.

### **Fire protection**

Fire detection installed in all different room. Extinguishing system deployed following "FM Global" recommendation. (Genset room, IT space, Some of the technical room).

- Smoke exhaust system installed for all different spaces, with capacity calculation online with the volume of the space.
- Characteristics of the wall, depending of the space, have an appropriate fire resistance.
- Genset and batteries rooms is 2 hours fire resistant. IT room are 1-hour fire resistant for buildings “design X” and 2 hours for buildings “design Y” & Y”

### **Flood**

For building equipped with chilled water system, there is no piping into technical rooms. All water loop located into the corridors, where are installed the CraC units. Roof and floors are all watertight. Technical corridors are equipped with a trap to collect water and evacuate directly to used water network.

### **Fire extinguishing system**

Fire extinguishing system installed depending on the type of room. IT space all equipped.

Extinguishing system are fully programmed and automated following "FM Global" recommendation.

- DCs "design X" are equipped with Nitrogen.
- DCs "design Y Y' & Y'" are equipped with Fog. Some of the technical rooms equipped with Sprinklers.

### **Main Power Supply High Voltage**

- High Voltage Supply in Marcoussis: 2 dedicated & direct underground electrical feeds in 90 kV directly connected to Villejust substation: 2 x 2 substation with High Voltage.
- Transformers which step down the power from 90 kV in 20 Kv
- different loops of 20 kV that feed each datacenter through 2 different ways
- The Dual site is fed by 2 substations in 20 kV – Two different energy suppliers: Marcoussis is powered by RTE and Dual Building powered by ENEDIS

### **Redundancy and UPS (Uninterrupted Power Supply)**

Double feed at transformer level. Switchboard are doubled and paired with each other.

For all IT space, UPS installed with batteries. Autonomy of the batteries is calculated to provide 10 Minutes full load.

Each chain of UPS and batteries are in a separated room.

All IT Rooms are powered by via two different chains of UPS

### **Power generator**

All building equipped with generators:

- Diesel engine for boat.
  - Building "design X" is N+2 (2500 kVA X 4)
  - Building "design Y & Y'" is N+1 (2500 kVA X 3)
  - Building "design Y'" is N+1 (3250 kVA X 8)
- The autonomy for each DC is 94 hours (100,000 liters in 2 tanks)

# 1 **BUILDING “ DESIGN X ”: Infrastructure description** DC01/DC02/DC03/DC04/DC07/DC08/Dual Building

## Design (Capacity 1.5 kW /sq.m)

- Building divided into 2 blocks (A & B)
- 4 x 250 sqm of IT rooms for customers on 2 floors (2 000 m² IT space)

## POWER – 2N Distribution

- Per block – 2 redundant electrical chains
- 2 x (2) Transformers of 3150 kVa 2N
- 6 x (3) UPS per bloc (1500 kva) 2N

## Centralized Backup at the building level

- 3 Generators backup (2500 kVa each) N+1
- 2 tanks for Fuel (50 000l each) 94 hours autonomy

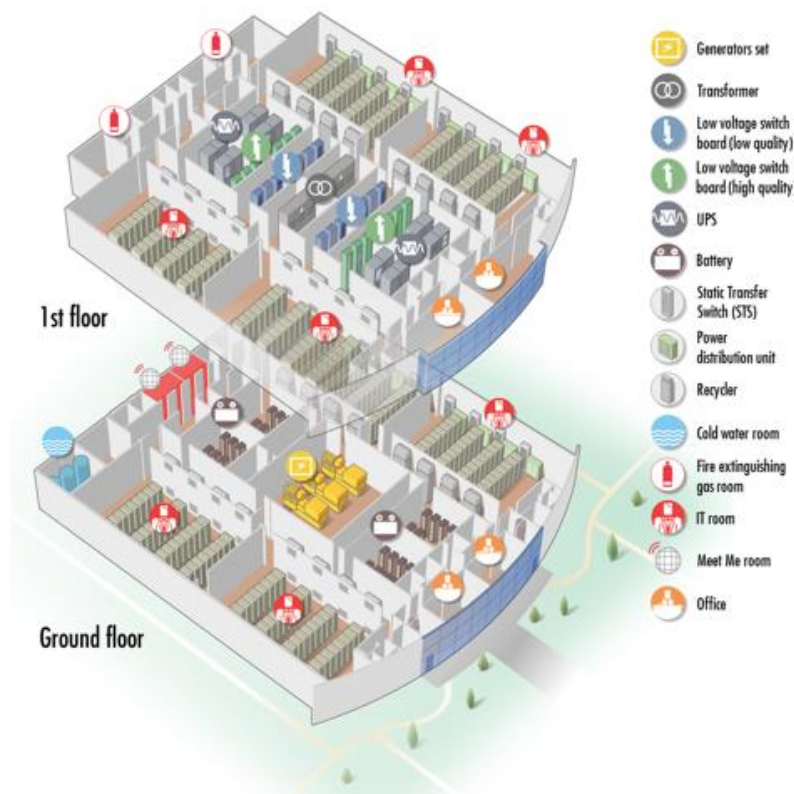
## Cooling

- 4 chillers (1100 kVa) N+1 at building level
- 6 CRAH per room (101 kWf each) N+2 at room level

## Fire Protection

- Double interlock pre-action Nitrogen
- Overhead smoke detection & HSSD

## Architecture's basic presentation



This report is intended solely for the information and use of Data4, customers of Data4 Hosting services, and the independent auditors of such customers.

## **2 BUILDING “ DESIGN Y ”: Infrastructure description (DC05/DC06/DC09/DC10).**

### **Modular Design (Capacity 1.8 kW / sq.m)**

- 2000 sq.m of IT rooms on 1 floor and divided into 2 main datahalls of 1000 sq.m each.
- Technical rooms located at the back of the building on 2 levels.
- Each technical function is isolated in a dedicated room

### **POWER – Shared distribution 3N/2**

- Principle: power is shared on 3 chains but 2 chains can take the full load
- 2 Transformers per Chain of UPS (2 000 Kva) 2N
- 3 chain of UPS- 4 UPS per chain (4500 kva) N+1

### **Power backup at the building level**

- 4 stand-by Generators back-up (2500 kVa each) N+2
- 2 tanks for Fuel (50 000l each) 94 hours autonomy

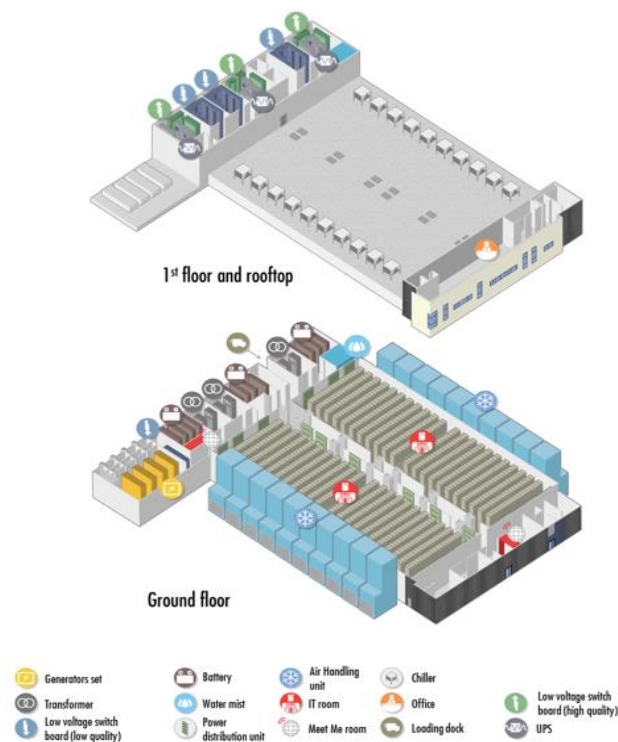
### **Cooling**

- Per Datahall/IT Room:
- 10 AHU per room (225 kwf each) FREE COOLING N+2
- (20 Air Handling Unit) N+4

### **Fire Protection**

- Double interlock pre-action Water Mist system
- Overhead smoke detection & HSSD

### **Architecture's basic presentation**



This report is intended solely for the information and use of Data4, customers of Data4 Hosting services, and the independent auditors of such customers.

### 3 **BUILDING “ DESIGN Y’ ” : Infrastructure description (DC11/DC12/DC14/DC15 / DC16 / DC17 / DC19).**

#### Modular Design (Capacity 2.0 kW / sq.m)

- 2000 sq.m of IT rooms on 1 floor and divided into 2 main datahalls of 1000 sq.m each.
- Technical rooms located at the back of the building on 2 levels.
- Each technical function is isolated in a dedicated room

#### POWER – Shared distribution 3 + 1

- Principle: power is shared on 3 chains but 1 chain can take the full load
- 1 transformer per Chain of UPS (2750 Kva) N+1
- 4 chain of UPS - 6 UPS (6 x 250 kva) per chain (4 x 1,5 MVA total) N+1

#### Power backup at the building level

- 4 stand-by Generators back-up (2500 kVa each) N+1
- 2 tanks for Fuel (50 000l each) 94 hours autonomy

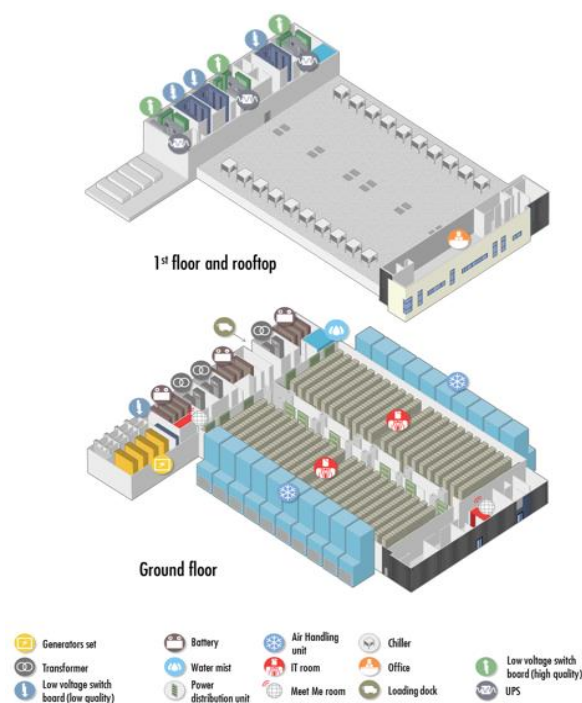
#### Cooling

- Per Datahall/IT Room:
- 10 AHU per room (300 kwf each) FREE COOLING INDIRECT N+2
- (20 Air Handling Unit) N+2

#### Fire Protection

- Double interlock pre-action Water Mist system
- Overhead smoke detection & HSSD

#### Architecture's basic presentation



This report is intended solely for the information and use of Data4, customers of Data4 Hosting services, and the independent auditors of such customers.

#### 4 BUILDING “DESIGN Y” : Infrastructure description (DC18 / DC20)

##### **Modular Design (Capacity 2.5 kW / sq.m)**

- 4000 sq.m of IT rooms on 2 floors and divided into 4 main datahalls of 1000 sq.m each.
- Technical rooms located on either side of the building on 2 levels.
- Each technical function is isolated in a dedicated room

##### **POWER – Shared distribution 2\*(3 + 1)**

- Principle: power is shared on 4 chains but 3 chains can take the full load
- 1 transformer per Chain of UPS (2900 Kva) N+1
- 8 chain of UPS – 5 UPS (5 x 400 kva) per chain (8 x 2 MVA total) N+1

##### **Power backup at the building level**

- 8 stand-by Generators back-up (3250 kVa each) N+1
- 8 tanks for Fuel (40 000 l each) 72 hours autonomy

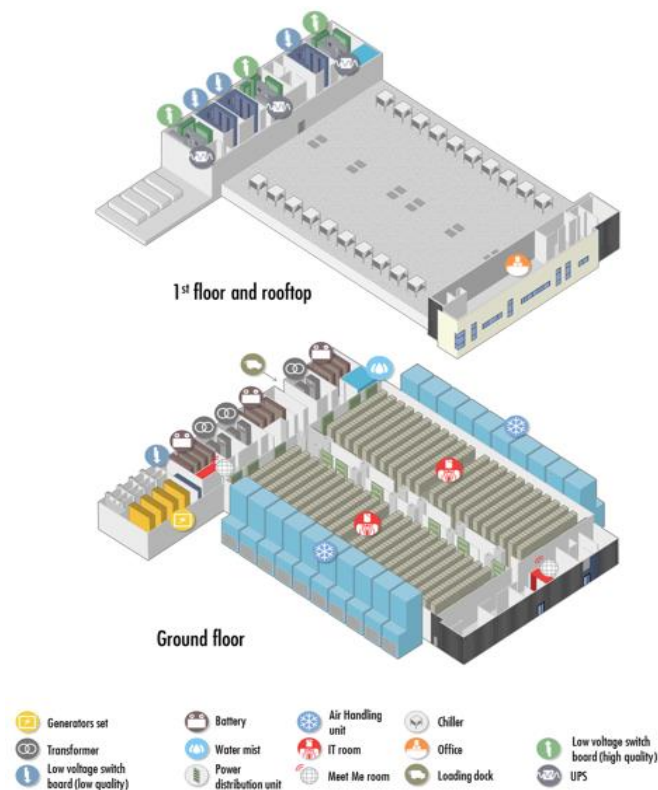
##### **Cooling**

- Per Datahall/IT Room:
- 12 Fanwalls per room (300 kwf each) FREE COOLING INDIRECT N+2
- 5 Air Handling Unit (for IT rooms) => 1 AHU in backup N+1

##### **Fire Protection**

- Double interlock pre-action Water Mist system
- Overhead smoke detection & HSSD

##### **Architecture’s basic presentation**



This report is intended solely for the information and use of Data4, customers of Data4 Hosting services, and the independent auditors of such customers.



**Information System/applications in use**

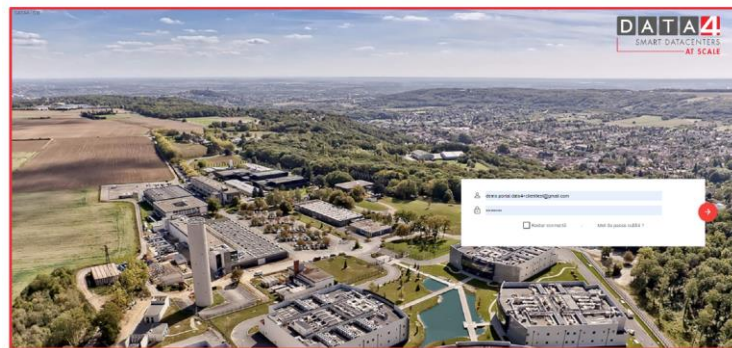
Data4 Services uses several tools as part of its activities, namely for the most important:

- **CWP portal**, the access request management tool allowing the company's customers to formalize requests to create, modify and delete access assigned to their environments.
- **CMMS** (Computerized Maintenance Management System), all devices (environmental protection and food) of buildings are covered by a multi-year maintenance schedule:
  - 2000 equipment referenced per building.
  - Preventive maintenance programmed for 13 months.

BMS: A building management system (BMS) solution is deployed in each building/datacenter. This system is responsible for managing (supervising) equipment managing air conditioning, energy or fire warning systems. If these platforms are autonomous to know that they are not dependent on each other, they are resilient within the same building (doubled) and the data collected by them are centralized to be made available in time to the teams in charge the operation and maintenance of data centers (FOC or Facility Operations Center) installed near the teams in charge of safety and security of the Marcoussis campus.

**PORTAIL CLIENT ou CWP (1/9)**

Page d'authentification du portail client (ou « Customer Web Portal »)



**D. Data Center operations and environmental controls**

**Physical Security**

The data center facilities are secured using a computerized proximity card-access system. The proximity card-access control system is used where access is controlled by time of day, day of week, and according to activity's justification. Additionally, the security system provides a record of entry, thus providing an audit of activity at the controlled doors, both perimeter and interior.

The access system controls electronic locks on both interior and exterior doors. The electronic locks on doors are active 24/7. Additionally, the facility is equipped with CCTV and a 24/7, third-party security service. Security guards monitor building entrances and one guard tours the premises regularly.

Guards complete a Daily Activity Report that details what events occurred at their particular post during the shift. If an incident occurs, the guard will note it in the report and complete an Incident Report. The supervisor of security, along with the security guard supervisor, reviews the reports on a daily basis, and Incident Reports are distributed to the manager of security.

Access controls are installed for exterior and interior doors, where needed. The proximity card-access control system is used so approved access is controlled by time of day, day of week and job function. The system also provides a history trail of access by card number and access point.

CCTV is deployed within the data center area and at strategic points throughout the building, floor or wing. CCTV also provides identification for cross-reference with the proximity access system of site movements.

Visitors are required to hand a piece of identity to the site. Visitors may receive an active temporary card-access if an authorized person has made the request. Other visitors receive identification badges for inactive visitors and are escorted into the facility by an authorized person. The inactive visitor ID badges are distributed on a per-day basis and expire at day's end.

The access system logs personnel who enter an interior or exterior door on a real-time basis. The security department will monitor the system logs for exceptions. Data4 managers review access lists of individuals with physical access to data centers at least annually to verify access to the site and to internal server rooms.

Access to the client computer rooms is managed, through the customer portal (CWP), by the client administrators declared to Data4 Services. Within the scope of responsibility of access to rooms delegated to the client, the administrators appointed by the customers are responsible for creating, modifying, or revoking access for their staff but also for their suppliers, partners or third parties (such as their own clients). Authorization reviews (access rights) are manageable by Data4 Services customers via the customer portal and accesses (activity logs) that can be fully communicated to the customer upon request to Data4 Services. The review of these accesses is very often integrated into service steering meetings organized very regularly with a large majority of our clients, always at their request.

#### **Access Security management**

A physical environment suitable to protect IT equipment and people from man-made and natural hazards has been established by the installation of environmental and physical controls that are regularly reviewed for their proper function.

Control procedures include identification of personnel and visitors, access to facilities, environmental threat protection, physical security and personnel safety.

Data4 Services's Managers team examine and approve personnel access to data centers and core rooms. For environment access managed under the responsibility of the Managed Services team, a recertification process is implemented, and a user access review is performed and properly documented once a year.

Also, Data4 Services's clients have in charge to performs regularly a user access badges for environment access managed under their responsibility.

With the access control system, the badges (permanent and temporary) are defined automatically or manually according to the form of the request (via the CWP web portal or the email). When the request is made on the CWP web portal or by email, Data4 Services ensures that the access configuration of the badge is consistent with the choices and environments defined.

#### **Environmental controls**

The data centers are equipped for the provision of power from the local/national power company; this supply is backed up by the on-site generator(s) designed to provide emergency power to hosted systems. The power is distributed via automatic transfer switches (ATSs), UPS systems and multiple power distribution units (PDUs).

The data center areas are supported by environmental systems (cooling and heating) that provide for a controlled environment to predefined parameters depending on the type, shape and model of the hosted equipment. The system consists of multiple air-handling units (AHUs) and includes redundancy to cover system failures or extreme conditions.

The facilities' infrastructures include power, power distribution and environmental controls for temperature and humidity, plus fire detection and suppression systems, which are monitored by Technical team 24/7.

This report is intended solely for the information and use of Data4, customers of Data4 Hosting services, and the independent auditors of such customers.



### **Monitoring**

Control center is managing and supervising the campus 24/7 in term of security and facility.

The monitoring equipment is located on-site but is monitored via a remote location on site. The monitoring systems provide alerts when the management thresholds are exceeded.

Each of the two teams (security and technical) log and report events where a threshold has been exceeded or an alert identified. The event are dispatched to a predetermined list of employees or a maintenance company. Dispatches are either by telephone, email or text.

The responsible employee be responsible for monitoring progress for the duration of the fault and for invoking escalations as required.

### **Fire Detection and Suppression**

Each of the data center's generation and server rooms are equipped with fire detection and suppression equipment. All technical rooms are equipped with smoke detectors, generators rooms are equipped also with flames detector and battery rooms are equipped with gas detectors.

The data centers utilize a highly sensitive smoke detector (HSSD) fire detection system along with heat detectors and uses an N2 gas fire suppression system.

### **Redundant Power**

The Marcoussis's data centers have a minimum of 72 hours fuel autonomy with their diesel generators. The data centers are equipped with dual power feeds, dual UPS system with 2N redundant configurations and diesel generators with N+1 redundancy.

### **Physical Alarm**

Fire and intrusion alarm systems are monitored 24/7. External doors to the data center area are alarmed in accordance with local health and safety guidelines; these alarms are controlled and recorded at either the central control facility or the local facility.

### **Climate Control**

Climate control equipment is installed at the Data4 Services's data centers to protect against environmental factors, such as heat and humidity. These systems are maintained on a regular basis.

### **Emergency Procedures and Routes**

Emergency procedures have been developed that encompass the various types of emergencies that could occur. Evacuation routes and exits are identified and posted in various locations in the facilities.

Emergency lighting is installed at data center facilities in the event of power failure or emergency. In addition, building management periodically conducts fire drills.

### **Preventive maintenance**

Third-party maintenance contracts exist for environmental systems, including the UPS, heating, ventilation and air conditioning (HVAC), and diesel generator. Operational procedures for power and environmental systems are provided and maintained by power and infrastructure.

Any intervention must be the subject of a validated application in the software (CMMS) with the formalization of an intervention report. Third party maintenance reports are archived on specific servers.

This report is intended solely for the information and use of Data4, customers of Data4 Hosting services, and the independent auditors of such customers.

#### **IV. Auditor’s description of system and controls**

During our visit on 16 & 17 November 2024 to the Marcoussis site, we visited the following Data Centers:

- DC04 of generation X ;
- DC05 of generation Y ;
- DC11 of generation Y’ ;
- DC20 of generation Y” ;

Each of these infrastructures represents DC generation. Thus, we covered all the generations of DC present on Marcoussis’s site:

- Generation X : DC01, DC02, DC03, DC04, DC07, DC08 and DB (Dual Building) ;
- Generation Y : DC05, DC06, DC09 and DC10 ;
- Generation Y’ : DC11, DC12 , DC14, DC15, DC16, DC17 and DC19 ;
- Generation Y” : DC18, DC20

Our examination of specific controls related to Data Centers provided by Data4 Services was limited to objectives control objectives and related controls specified by Data4 Services in Section III.

It did not include the procedures in place at user organizations or other procedures which may be described, but not identified, in the specific controls and tests of controls as outlined in this section of the report.

A description of the type of tests, performed for the operational effectiveness of the controls detailed in the following matrices, is described below :

**Type of Test Procedures Performed**

TYPE	DESCRIPTION
<b>Inquiry</b>	<p>Inquire of appropriate personnel seeking relevant information or representation including among other things:</p> <ul style="list-style-type: none"> <li>▪ Knowledge and additional information regarding the policy or procedure</li> <li>▪ Corroborating evidence of the policy or procedure</li> </ul> <p>As inquiries were performed for substantially all controls, the test was not listed individually for every control shown in the accompanying matrices.</p>
<b>Observation</b>	Observe the application or existence of specific controls as represented.
<b>Inspection</b>	<p>Inspect documents and records indicating performance of the controls. This testing includes among other things:</p> <ul style="list-style-type: none"> <li>▪ Inspection of reconciliations and management reports that age or quantify reconciling items to assess whether balances and reconciling items are properly monitored, controlled and resolved on a timely basis</li> <li>▪ Examinations of source documentation and authorizations to verify propriety of transactions processed</li> <li>▪ Examination of documents or records for evidence of performance, such as existence of initials or signatures</li> <li>▪ Inspection of systems documentation, such as operations manuals, flow charts and job descriptions</li> </ul>
<b>Re-performance</b>	<p>Re-perform the control, or processing of the application controls, to help ensure the accuracy of its operation. This testing includes, among other things:</p> <ul style="list-style-type: none"> <li>▪ Obtaining evidence of the arithmetical accuracy and correct processing of transactions by performing independent calculations</li> <li>▪ Re-performing the matching of various system records by independently matching the same records and comparing reconciling items to the Company's prepared reconciliations if applicable.</li> </ul>

## SECTION IV. AUDITOR'S DESCRIPTION OF SYSTEM AND CONTROLS

Section	Title of control	Control N°	Control Description	Testing Performed by Grant Thornton	Test results
Physical Security	Site access Buildings	1.1	<b>Site access Buildings</b>  Access to the site and to other buildings are covered by a daylight reception/security personnel and is there a team security assuring 24/24 7/7 guarding.	<b>Observation</b>  1- Observed on the Marcoussis site that a temporary card-access is required against an identity document for visitors. The safety instructions are posted on the site.  <b>Inspection</b>  2- Verified that the assigned card-access are nominative and tested the accesses are limited and configured according to the request.  3- Verified that a contract with a supplier is signed for 2024 in order to set up a security team assuring 24/24 7/7 guarding.	No exceptions noted
	Server/computer room access	1.2	<b>Server/computer room access</b>  There are 3 access control zones (Campus" Zone, "DC" Zone and «DC Interior" Zone) before access to computer rooms:  <ul style="list-style-type: none"> <li>• Security check : Limited access by card-access (permanent or temporary).</li> <li>• Safety grid around the zone's perimeter.</li> <li>• CCTV controls.</li> <li>• Access by unipersonal airlock (human or vehicle).</li> </ul>	<b>Observation</b>  1. Observed during the Marcoussis site visit that security facilities exist at each level of "access" zone. The data center facilities are secured using a computerized proximity card-access system.  <b>Inspection</b>  2. Selected four Datacenters of different generations, verified the existence of security facilities (CCTV, access control system, card-access...), and ensured that they are supervised from the center control.  3. Access controls are installed for exterior and interior doors. The access system controls electronic locks on both interior and exterior doors. The system also provides a history trail of access by card number and access point.	No exceptions noted
	Technical local access	1.3	<b>Technical local access</b>  The technical rooms in the data centers are accessible with keys managed and controlled by a secure electronic safe (with a password login).	<b>Inspection</b>  1. Verified that the electronic safe keeping the keys allowing access to the technical rooms, logs in real time the accesses and the key's users.	No exceptions noted

## SECTION IV. AUDITOR'S DESCRIPTION OF SYSTEM AND CONTROLS

Section	Title of control	Control N°	Control Description	Testing Performed by Grant Thornton	Test results
Environ mental controls	Environment al risks	2.1	<p><b>Environmental risks</b></p> <p>An environmental risk analysis is done on the external and internal risks (pollution, flood, earthquake, social movement, forest fire, physical safety problem, monitoring unavailability, weather unavailability, network failure etc ...).</p> <p>This process is part of the ISO 14001 certification.</p>	<p><b>Observation</b></p> <p>1. Observed the Environmental Risk Matrix formalizes the risk assessment and coverage measures, that are regularly reviewed for their suitability.</p>	No exceptions noted
	Prevention/ Detection facilities	2.2	<p><b>Prevention/detection facilities</b></p> <p>Fire detection + HSSD (Vesda) High Sensitivity Smoke Detection facilities Humidity sensors - ambiance (atmospheric) Temperature sensors atmospheric and returned air.</p> <p>Public areas are covered by video surveillance, private (customers') spaces on demand.</p>	<p><b>Inspection</b></p> <p>1. Visited four datacenters of different generations and verified the existence of fire prevention / detection facilities are installed on the entire building with a system of locating possible disaster areas.</p>	No exceptions noted
	Air conditioning /cooling systems	2.3	<p><b>Air conditioning/cooling systems</b></p> <p>Air conditioning facilities have N+1 or N+2 level of redundancy. The air conditioning facilities and infrastructures are located outside the servers/customers' rooms - but inside the building, in the technical corridors.</p>	<p><b>Inspection</b></p> <p>1. Visited four datacenters of different generations and verified the existence of the cooling facilities in rooms with redundancy.</p> <p>2. For each of the air conditioning system units of the selected data centers, reviewed maintenance reports for 2024 prevent water leakage.</p>	No exceptions noted
	Fire protection	2.4	<p><b>Fire protection</b></p> <p>Fire detection installed in all different room. Extinguishing system deployed following "FM Global" recommendation. (Genset room, IT space, Some of the technical room)</p> <p>Smoke exhaust system installed for all different spaces, with capacity calculation online with the volume of the space.</p> <p>Characteristics of the wall, depending on the space, have an appropriate fire resistance.</p> <p>Genset and batteries rooms is 2 hours fire resistant. IT room are 1 hour fire resistant.</p>	<p><b>Inspection</b></p> <p>1. Visited four different generation datacenters and verified that the buildings and rooms actually meet the fire resistance and reaction to fire characteristics (double fire doors ...).</p> <p>2. For each unit of the fire detection facilities, reviewed that the maintenance reports of 2024 ensure their performance.</p>	No exceptions noted

## SECTION IV. AUDITOR'S DESCRIPTION OF SYSTEM AND CONTROLS

Section	Title of control	Control N°	Control Description	Testing Performed by Grant Thornton	Test results
Environmental controls	Flood	2.5	<b>Flood</b>  For building equipped with chilled water system, there is no piping into technical rooms. All water loop located into the corridors, where are installed the CraC units. Roof and floors are all watertight. Technical corridors are equipped with a trap to collect water and evacuate directly to used water network ("wastewater").	<b>Inspection</b>  1. Visited four datacenters of different generations and verified the existence of the facilities of recovery and evacuation of water in case of flood, ensuring the absence of failure of pipe and drains.	No exceptions noted
	Fire extinguishing system	2.6	<b>Fire extinguishing system</b>  Fire extinguishing system installed depending on the type of room. It spaces all equipped.  Extinguishing systems are fully programmed and automated following "FM Global" recommendation.  First generation of DC is equipped with Nitrogen. All other generation are equipped with Fog. Some of the technical rooms equipped with Sprinklers.	<b>Inspection</b>  1. Visited four datacenters of different generations and verified the existence of the automatic fire extinguishing system in several places in the corridors.  2. For each of the selected data centers, reviewed the maintenance reports of 2024 and verified that fire extinguishers are regularly tested and changed.	No exceptions noted
	Monitoring	2.7	<b>Monitoring</b>  Two different teams dedicated for alarm and supervision: - Security control center is managing and supervising the campus 24/7 in term of security + fire man brigade on site. - Technical team to supervise facilities 24/7. On call services for both activity: Security and Facility.	<b>Inspection</b>  1. Observed the datacenter's supervision center and verified that all protection and power supply systems are covered by the monitoring board, permanently 24/7.  Security and technical alerts are logged in live, as well as the management of their treatments.	No exceptions noted

## SECTION IV. AUDITOR'S DESCRIPTION OF SYSTEM AND CONTROLS

Section	Title of control	Control N°	Control Description	Testing Performed by Grant Thornton	Test results
<b>Power supply</b>	Electrical power	3.1	<b>Electrical power</b>  Campus is powered via 2 dedicated cables from substation (RTE) directly to the campus (90 kV).	<b>Observation</b>  1. Observed technical architecture records of Datacenters (old and new generation), ensuring the existence of at least two main power sources.  2. We consult the original contract and the 2020 amendment with RTE which clearly indicates that the campus is supplied via 2 dedicated 90 kV cables.	<b>No exceptions noted</b>
	Redundancy and UPS (Uninterrupted Power Supply)	3.2	<b>Redundancy and UPS</b>  Double feed at transformer level. Switchboard are doubled and paired with each other. For all IT space, UPS installed with batteries. Capacity of the UPS determine the acceptable load for each space. Autonomy of the batteries is calculated to provide 10 Minutes full load. Each chain of UPS is in a separated room. The same for battery.	<b>Inspection</b>  1. Visited four datacenters of different generations and verified the existence of UPS, distant from each other.  2. For each of the selected data centers, reviewed the maintenance report of 2024, ensured that the UPS system is redundant with a sufficient autonomy capacity to cover all the infrastructures.	<b>No exceptions noted</b>
	Power generator	3.3	<b>Power generator</b>  All building equipped with generators. Diesel engine for boat. - Generation X is 2500 kVA x 3 - Generations Y, Y' and Y'' are 2500 kVA x 4 Theoretical autonomy for all DC is 94 hours (100 000 liters in 2 tanks).	<b>Inspection</b>  1. Visited four Datacenters of different generations and verified the existence of the generators with the diesel engine of boat.  2. For each of the selected data centers, reviewed the maintenance report of 2024, ensured that the generators have sufficient power rating to meet the datacenter requirements.	<b>No exceptions noted</b>

## SECTION IV. AUDITOR'S DESCRIPTION OF SYSTEM AND CONTROLS

Section	Title of control	Control N°	Control Description	Testing Performed by Grant Thornton	Test results
User access management	Client Web Portel (CWP). - identification et authentication	4.1	<b>Client Web Portal (CWP). - identification et authentication</b>  Access to the CWP Portal is managed through an individual user account and authentication mechanisms in accordance with best practices (use of password).	<b>Inspection</b>  1. Ensured that access to the CWP portal respected good practices in terms of setting passwords (length, attempts, expiration time, ...).	<b>No exceptions noted</b>
	Customer Web Portel (CWP). – user recertification	4.2	<b>Customer Web Portal (CWP). – user recertification</b>  A review of DATA4 staff clearance is conducted annually by security team in France. The review is made for all country (Poland, Spain, Italy and France). The review is made in Excel document. A Jira ticket is created for each account identified as an anomaly.	<b>Inspection</b>  1. Verified the existence of the latest user access recertifications on CWP in 2024.	<b>No exceptions noted</b>
	Genetec - Access management	4.3	<b>Genetec - identification and authentication</b>  Access to Genetec is managed through an individual user account and authentication mechanisms in accordance with best practices (use of password).	<b>Inspection</b>  1. Ensured that access to Genetec respected good practices in terms of setting passwords (length, attempts, expiration time, ...).	<b>No exceptions noted</b>
	Genetec – Physical access	4.4	<b>Genetec - physical access</b>  A review of employees with access to SOC is carried out annually by security team. The review is made in Excel document. An investigation is conduct for each anomaly.	<b>Inspection</b>  1. Verified the existence of the last review of agents with access to the SOC carried out in 2024.	<b>Exceptions noted</b>  No review of physical access to the SOC was carried out in 2024 by the physical security team.  The "exceptions noted"'s impact is limited . A review of SOC access was carried out by Data4 on 02/12/2024. No anomalie was identified.



## SECTION IV. AUDITOR'S DESCRIPTION OF SYSTEM AND CONTROLS

Section	Title of control	Control N°	Control Description	Testing Performed by Grant Thornton	Test results
	Genetec – User recertification	4.5	<b>Genetec – user recertification</b>  A review of employees with access to Genetec is carried out annually by security team. The review is made in Excel document. An investigation is conduct for each anomaly.	<b>Inspection</b>  1. Verified the existence of the latest user access recertifications on Genetec in 2024.	<b>No exceptions noted</b>
	Datacenters - Access management	4.6	<b>Datacenters - Access management</b>  With the access control system (Genetec), the card-access (permanent and temporary) are set automatically according to the environments defined by the customer, when he requests it on the CWP portal.  In case of requests made by mail. The access configuration is done directly in the Genetec software.  A review of the physical access granted in Genetec is carried out monthly on a sample of 20 requests. The review is made in Excel document. An investigation is conduct for each anomaly.	<b>Observation</b>  1. Observed an access creation request formulation in the software and verified that the user had authorization rights (to data centers and server rooms) limited to the signed contractual agreements.  <b>Inspection</b>  2. Verified that the access control system configured rights of the card-access according to the CWP request.	<b>No exceptions noted</b>

## SECTION IV. AUDITOR'S DESCRIPTION OF SYSTEM AND CONTROLS

Section	Title of control	Control N°	Control Description	Testing Performed by Grant Thornton	Test results
<b>Preventive maintenance</b>	Proof of maintenance or tests	5.1	<p><b>Proof of maintenance or tests</b></p> <p>All facilities (environmental protection and food) of buildings are covered by a multi-year maintenance schedule.</p> <p>Any intervention must be the subject of a validated application in the software (CMMS) with the formalization of an intervention report.</p> <p>Third party maintenance reports are archived on specific servers.</p>	<p><b>Inspection</b></p> <p>1. Verified the existence of multi-year maintenance schedule for all facilities.</p> <p>2. Verified that all critical maintenance reports are available and formalized.</p> <p>3. Verified that all interventions produced a formalized report.</p> <p>4. Verified that all reports are centralized by Data 4.</p> <p>5. Verified that the CMMS tool implemented manage maintenance reports.</p>	<p><b>Exceptions noted</b></p> <p>The CMMS tool implemented does not manage maintenance reports.  <i>NB : In 2025, Data4 plans to change tools (from SAMFM to MCIM). This new tool will be used to manage maintenance reports.</i></p> <p>The "exceptions noted"'s impact is limited .  All maintenance's reports have been found and seen during the audit.</p>

## V. Other information provided by Data4 Services

### ISO certifications

The following certificates illustrate current ongoing Data4 Services ISO certifications.

- ISO/IEC 27001: 2013



Bureau Veritas Certification

**DATA 4 SERVICES**

6 RUE DE LA TREMOILLE  
75008 PARIS  
FRANCE

This is a multi-site certificate, additional site(s) are listed on the next page(s)

*Bureau Veritas Certification Holding SAS – UK Branch certifies that the Management System of the above organisation has been audited and found to be in accordance with the requirements of the management system standards detailed below*

---

**ISO/IEC 27001:2013**

*Scope of certification*

---

**INFORMATION SECURITY MANAGEMENT SYSTEM FOR  
SECURED HOSTING OF IT INFRASTRUCTURE**

*Statement of Applicability Version number and release date:  
v1.3 of 20/10/2021*

Original cycle start date:	<b>03 February 2016</b>
Expiry date of previous cycle:	<b>02 February 2022</b>
Certification / Recertification Audit date:	<b>13 January 2022</b>
Certification / Recertification cycle start date:	<b>03 February 2022</b>

Subject to the continued satisfactory operation of the organization's Management System, this certificate expires on: **02 February 2025**

<b>Certificate No.</b>	<b>FR072348</b>	<b>Version: 1</b>	<b>Issue date: 17 January 2022</b>
<b>Previous Certificate No.</b>	<b>IND.19.6570/U</b>		
<b>Contract No.</b>	<b>12420141</b>		



**Laurent CROGUENEC - President**  
**Signed on behalf of BVCH SAS UK Branch**




0008

Certification body address: 5<sup>th</sup> Floor, 66 Prescott Street, London E1 8HG, United Kingdom.  
Local office: Bureau Veritas Certification France : 9, cours du Triangle - CS 40100, 92937 Paris-La-Défense Cedex – France

Further clarifications regarding the scope of this certificate and the applicability of the management system requirements may be obtained by consulting the organisation.  
To check this certificate validity please call: + 33(0) 1 41 97 00 60.

This report is intended solely for the information and use of Data4, customers of Data4 Hosting services, and the independent auditors of such customers.

- ISO 9001: 2015



**DATA 4 SERVICES**

*Il s'agit d'un certificat multi-site, le détail des sites est énuméré dans l'annexe de ce certificat*

6 RUE DE LA TREMOILLE  
75008 - PARIS 8, FRANCE

*Bureau Veritas Certification France certifie que le système de management de l'organisme susmentionné a été audité et jugé conforme aux exigences de la norme :*

*Standard*

---

**ISO 9001:2015**

*Domaine d'activité*

---

**DEVELOPPEMENT ET COMMERCIALISATION DE SOLUTIONS  
D'HEBERGEMENT INFORMATIQUE SECURISE ET MAINTIEN  
EN CONDITION OPERATIONNELLE DES INFRASTRUCTURES  
DATA CENTER.**

**DEVELOPMENT AND COMMERCIALIZATION OF SECURED IT HOSTING  
OF IT INFRASTRUCTURE AND MAINTENANCE IN OPERATIONAL  
CONDITIONS OF DATA CENTER INFRASTRUCTURES.**

Date d'entrée en vigueur : **02 mars 2022**

Sous réserve du fonctionnement continu et satisfaisant du système de management de l'organisme, ce certificat est valable jusqu'au : **17 février 2025**



Certificat n° : **FR072759-1** Date: **03 mars 2022**

Affaire n° : **12418855**


**Laurent CROGUENEC - Président**

Adresse de l'organisme certificateur : Bureau Veritas Certification France  
Le Triangle de l'Arche - 9 Cours du Triangle - 92937 Paris La Défense

Des informations supplémentaires concernant le périmètre de ce certificat ainsi que l'applicabilité des exigences du système de management peuvent être obtenues en consultant l'organisme.  
Pour vérifier la validité de ce certificat, vous pouvez téléphoner au : **+ 33 (0)1 41 97 00 60.**



- ISO 14001: 2015



**DATA 4 SERVICES**

*Il s'agit d'un certificat multi-site, le détail des sites est énuméré dans l'annexe de ce certificat*

6 RUE DE LA TREMOILLE  
75008 - PARIS 8, FRANCE

*Bureau Veritas Certification France certifie que le système de management de l'organisme susmentionné a été audité et jugé conforme aux exigences de la norme :*

*Standard*

---

**ISO 14001:2015**

*Domaine d'activité*

---

**DEVELOPPEMENT ET COMMERCIALISATION DE SOLUTIONS  
D'HEBERGEMENT INFORMATIQUE SECURISE ET MAINTIEN  
EN CONDITION OPERATIONNELLE DES INFRASTRUCTURES  
DATA CENTER.**

**DEVELOPMENT AND COMMERCIALIZATION OF SECURED IT HOSTING  
OF IT INFRASTRUCTURE AND MAINTENANCE IN OPERATIONAL  
CONDITIONS OF DATA CENTER INFRASTRUCTURES.**

Date d'entrée en vigueur : **02 mars 2022**

Sous réserve du fonctionnement continu et satisfaisant du système de management de l'organisme, ce certificat est valable jusqu'au : **17 février 2025**



Certificat n° : **FR072761-1**      Date: **03 mars 2022**

Affaire n° : **12418855**

**Laurent CROGUENNEC - Président**

Adresse de l'organisme certificateur : Bureau Veritas Certification France  
Le Triangle de l'Arche - 9 Cours du Triangle - 92937 Paris La Défense

Des informations supplémentaires concernant le périmètre de ce certificat ainsi que l'applicabilité des exigences du système de management peuvent être obtenues en consultant l'organisme.  
Pour vérifier la validité de ce certificat, vous pouvez téléphoner au : + 33 (0)1 41 97 00 60.





- ISO 50001: 2018



**DATA 4 SERVICES**

*Il s'agit d'un certificat multi-site, le détail des sites est énuméré dans l'annexe de ce certificat*

SIREN N° : 49325464300031  
6 RUE DE LA TREMOILLE  
75008 – PARIS 8, FRANCE

*Bureau Veritas Certification certifie que le système de management de l'organisme susmentionné a été audité et jugé conforme aux exigences de la norme :*

---

*Standard*

**ISO 50001 : 2018**

---

*Domaine d'activité*

**DEVELOPPEMENT ET COMMERCIALISATION DE SOLUTIONS D'HEBERGEMENT INFORMATIQUE SECURISE ET MAINTIEN EN CONDITION OPERATIONNELLE DES INFRASTRUCTURES DATA CENTER.**

**DEVELOPMENT AND COMMERCIALIZATION OF SECURED IT HOSTING OF IT INFRASTRUCTURE AND MAINTENANCE IN OPERATIONAL CONDITIONS OF DATA CENTER INFRASTRUCTURES.**

*Le domaine certifié couvre l'ensemble des activités des sites en annexe hors site centralisateur.*

Date d'entrée en vigueur : **10 mars 2022**

Sous réserve du fonctionnement continu et satisfaisant du système de management de l'organisme, ce certificat est valable jusqu'au : **09 mars 2025**

Date originale de certification : **09 mars 2016**

Certificat n° : **FR073365-1**      Date: **11 mars 2022**

Affaire n° : **12419345**

**Laurent CROGUENEC - Président**

Adresse de l'organisme certificateur : Bureau Veritas Certification France  
Le Triangle de l'Arche - 9 Cours du Triangle - 92937 Paris La Défense

Des informations supplémentaires concernant le périmètre de ce certificat ainsi que l'applicabilité des exigences du système de management peuvent être obtenues en consultant l'organisme. Pour vérifier la validité de ce certificat, vous pouvez téléphoner au : **+ 33 (0)1 41 97 00 60**.



- ISO 45001: 2018



**DATA 4 SERVICES**

*This is a multi-site certificate, additional site details are listed in the appendix to this certificate*

6 RUE DE LA TREMOILLE  
75008 - PARIS 8, FRANCE

*Bureau Veritas Certification Holding SAS – UK Branch certify that the Management System of the above organisation has been audited and found to be in accordance with the requirements of the management system standards detailed below*

*Standard*

---

**ISO 45001:2018**

*Scope of certification*

---

**DEVELOPMENT AND COMMERCIALIZATION OF SECURED IT HOSTING OF IT INFRASTRUCTURE AND MAINTENANCE IN OPERATIONAL CONDITIONS OF DATA CENTER INFRASTRUCTURES.**

**DEVELOPPEMENT ET COMMERCIALISATION DE SOLUTIONS D'HEBERGEMENT INFORMATIQUE SECURISE ET MAINTIEN EN CONDITION OPERATIONNELLE DES INFRASTRUCTURES DATA CENTER.**

Original cycle start date: **7 March 2019**

Expiry date of previous cycle: **17 February 2022**

Certification / Recertification Audit date: **12 January 2022**

Certification / Recertification cycle start date: **7 March 2022**

Subject to the continued satisfactory operation of the organization's Management System, this certificate expires on: **6 March 2025**

Certificate No : **FR072762** - Version 1

File No : **12418855**

Revision Date : **7 March 2022**



**Laurent CROGUENNEC - President,**  
**Signed on behalf of BVCH SAS UK Branch**



0008

Certification body address: 66 Prescott Street, London E1 8HG, United Kingdom.  
Local office: Bureau Veritas Certification France : Le Triangle de l'Arche - 9 Cours du Triangle - 92937 Paris La Défense  
Further clarifications regarding the scope of this certificate and the applicability of the management system requirements may be obtained by consulting the organisation.  
To check this certificate validity please call + 33(0) 1 41 97 00 60.

## Other security certifications

The following certificates illustrate current ongoing Data4 Services additional security-related certifications.

- HDS v1.1: Juin 2018



This report is intended solely for the information and use of Data4, customers of Data4 Hosting services, and the independent auditors of such customers.



- PCI-DSS for Service Providers Version – April 2024

DocuSign Envelope ID: B1116472-B210-45EE-A32C-C973644A1599



## **PCI DSS v4.0 Attestation of Compliance for Report on Compliance – Service Providers**

**Entity Name: DATA4 France**

**Assessment End Date: 2024/03/28**

**Date of Report as noted in the Report on Compliance: 2024/04/17**