

# Organizational model for the protection of personal data

Revision: 1

**Date**: 10 May 2023 **Status**: Approved

PREPARED BY: PARTNERS4INNOVATION S.R.L. REVIEW BY: LEGAL AREA / PEOPLE AREA / IT AREA APPROVED BY: BOARD OF DIRECTORS



# **TABLE OF CONTENTS**

1.	INTRODUCTION	5
1.1	Characteristic Elements	5
1.2	Corporate notes	5
2	Scope	5
3	Field of Application	5
4	Terms and Definitions	6
5	Regulatory requirements	7
6	Organizational Model	9
6.1	Data Protection Committee	9
6.2	Data Protection Coordinator	10
6.3	Data Protection Referents	11
6.4	Data Protection Officer	12
6.5	Subjects Authorized to Process	13
6.6	System Administrators	14
6.7	Other players involved	14
7	Annexes	15

# INTRODUCTION

#### 1. INTRODUCTION

#### 1.1 CHARACTERISTIC FLEMENTS

Company Name (Parent Company): D-Orbit S.p.A.

Registered and administrative office:

V.le Risorgimento n. 57 - 22073 Fino Mornasco (CO)

VAT No.: 07373150965

Registration CCIAA Como - Lecco - REA 315886 PEC: d-orbit@pec.deorbitaldevices.com

#### 1.2 CORPORATE NOTES

The Company's object is:

- Research, conception, realization, development, production, marketing, leasing, loan and technical
  assistance of automated and/or semi-automated machines, electrical and electronic components, software
  and internet platforms, propulsion systems and control equipment, as well as aerospace satellite platforms
  and subsystems.
- Integration and delivery of on-orbit release, space transportation, and general satellite services.

#### 2 SCOPE

The purpose of this document is to describe the organizational model adopted to ensure adequate protection of Personal Data by D-Orbit S.p.A. (hereinafter "D-Orbit"), which includes the following companies:

- D-Orbit S.p.A. (Italy);
- D-Orbit Portugal (Portugal);
- D-Orbit UK Ltd (UK);
- D-Orbit Inc (USA).

### 3 FIELD OF APPLICATION

This document applies to all individuals, internal and external, who process Personal Data on behalf of D-Orbit, fulfilling one or more of the roles provided for within the organizational model.

# **4 TERMS AND DEFINITIONS**

Prerequisite	Description
Supervisory Authority	Independent public authorities charged in individual EU countries with overseeing the implementation of the GDPR in order to protect the fundamental rights and freedoms of data subjects (in Italy, the "Garante per la protezione dei Dati Personali").
Recipient	Natural or legal person, public authority or other body receiving communication of Personal Data, whether or not it is a third party.
Data Subjects	Individuals to whom the Personal Data refer.
Personal Data	Any information relating to an identified or identifiable natural person ("data subject").
General Data Protection Regulation (o "GDPR")	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
Processing	Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

# **5 REGULATORY REQUIREMENTS**

Below are the main regulatory requirements under the GDPR and Legislative Decree 196/2003, as amended and adapted to the GDPR by Legislative Decree 101/2018 (hereinafter, the "Revised Privacy Code") regarding the roles to be provided within the organizational model for the protection of Personal Data.

Prerequisite	Description	
	The Data Controller and the Data Processor shall designate a data protection officer in any case where:	
	the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;	
DPO - Mandatory	the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or	
Conditions (Art. 37, para. 1-4, GDPR)	<ul> <li>the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 and personal data relating to criminal convictions and offences referred to in Article 10.</li> </ul>	
	In other cases, Data Controller, Data Processor or associations and other bodies representing categories of controllers or processors may or, where required by Union or Member State law shall, designate a data protection officer. The data protection officer may act for such associations and other bodies representing Controllers or Processors.	
DPO - Quality, skills and capabilities (Art. 37, para.	Il The data protection officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in Article 39	
5, GDPR; Art. 38, para. 5, GDPR)	The data protection officer shall be bound by secrecy or confidentiality concerning the performance of his or her tasks, in accordance with Union or Member State law.	
DPO - Internal or external figure (Art. 37, para.6, GDPR)	The data protection officer may be a staff member of the controller or processor, or fulfil the tasks on the basis of a service contract.	
DPO - Contact Details (Art. 37, para.7, GDPR)	The controller or the processor shall publish the contact details of the data protection officer and communicate them to the supervisory authority.	
	The Data Controller and the Data Processor:	
	shall ensure that the data protection officer is involved, properly and in a timely manner, in all issues which relate to the protection of personal data;	
DPO - Position (art. 38,	shall support the data protection officer in performing the tasks referred to in Article 39 by providing resources necessary to carry out those tasks and access to personal data and processing operations, and to maintain his or her expert knowledge;	
para. 1,2,3,6, GDPR)	shall ensure that the data protection officer does not receive any instructions regarding the exercise of those tasks. He or she shall not be dismissed or penalised by the controller or the processor for performing his tasks. The data protection officer shall directly report to the highest management level of the controller or the processor.	
	The data protection officer may fulfil other tasks and duties. The controller or processor shall ensure that any such tasks and duties do not result in a conflict of interests.	

Prerequisite	Description
	The data protection officer shall have at least the following tasks:
	<ul> <li>to inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union or Member State data protection provisions;</li> </ul>
DPO - Duties (Art. 39,	<ul> <li>to monitor compliance with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;</li> </ul>
GDPR)	<ul> <li>to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 35;</li> </ul>
	to cooperate with the supervisory authority;
	<ul> <li>to act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36, and to consult, where appropriate, with regard to any other matter.</li> </ul>
	The data protection officer shall in the performance of his or her tasks have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.
DPO - Contact for data subjects (art. 38, co. 4, GDPR)	Data subjects may contact the data protection officer with regard to all issues related to processing of their personal data and to the exercise of their rights under this Regulation.
<b>Data Processor</b> (Art. 28, para. 1 GDPR)	Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.
Sub-Processor (Art. 28, para. 2, GDPR)	The processor shall not engage another processor without prior specific or general written authorisation of the controller. In the case of general written authorisation, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes.
	The processor and any person acting under the authority of the controller or of the processor, who has access to personal data, shall not process those data except on instructions from the controller, unless required to do so by Union or Member State law (Article 29 of the GDPR).
<b>Authorized</b> (Art. 29, GDPR and art. 2-quaterdecies, revised Privacy Code)	The Data Controller or the Data Processor may provide, under their own responsibility and within their own organizational structure, that specific tasks and functions related to the Processing of Personal Data be assigned to individuals, expressly designated, who operate under their authority. The Data Controller or the Data Processor shall identify the most appropriate ways to authorize persons operating under their direct authority to the Processing of Personal Data (Article 2-quaterdecies of the revised Privacy Code).
	Thus, the Authorized Persons for Processing are all employees operating under the direct authority of the structures appointed by the Data Controller for the management of data protection in compliance with the further instructions given and for the performance of the tasks entrusted to them, pursuant to Article 29 of the GDPR and Article 2-quaterdecies of Legislative Decree 196/2003, as amended and adapted to the GDPR by Legislative Decree 101/2018.

#### **6 ORGANIZATIONAL MODEL**

D-Orbit has adopted a set of structures, committees, and roles to ensure adequate protection of Personal Data, in compliance with obligations under Personal Data protection regulations and practices.

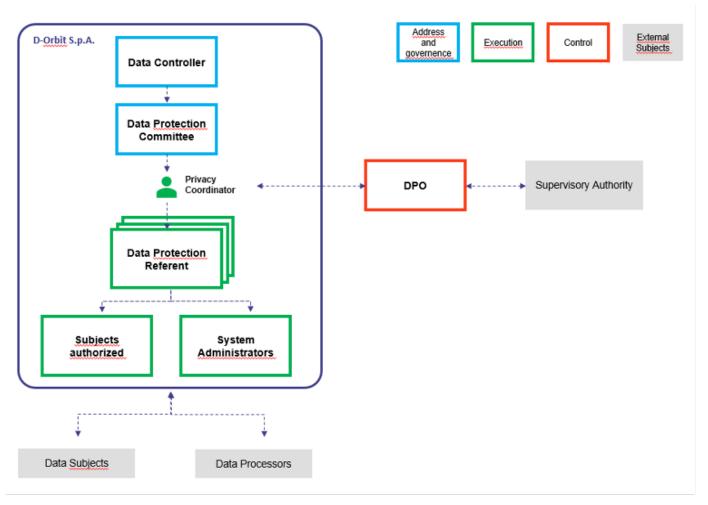


Figure 1 - Organizational model for the protection of Personal Data

The following paragraphs elaborate on the responsibilities assigned to each structure/role provided within the organizational model.

#### 6.1 DATA PROTECTION COMMITTEE

The Data Protection Committee, composed of specially empowered individuals such as the Chief Information Officer, the Chief People Officer and the General Counsel (or Legal Counsel his delegate), is an "on-demand" structure having a key role in the direction and governance of the Model for the Protection of Personal Data. Specifically, the Data Protection Committee is responsible for:

- define/update, with the support of the Data Protection Referent and supporting Functions, the Model and any other internal provisions on the protection of Personal Data;
- meet periodically, and in any case to the extent of not less than four times a year in close proximity to the quarterly Boards of Directors, or as convened by the Data Protection Coordinator or DPO to:
  - verify the level of compliance with Personal Data protection regulations and practices;
  - assess the risks of non-compliance related to Personal Data protection regulations and practices;
  - define and monitor the implementation of appropriate preventive and/or corrective actions to mitigate risks;
  - propose and execute training activities in favor of employees, proposing possible additions, to the whole population or to individual areas, due to specific events;

- manage and address critical events (e.g., stakeholder requests, breaches of Personal Data), submitting them to the attention/approval of the B.o.D. as necessary;
- suggest possible implementations to subsisting documentation, where assessed as necessary or appropriate in light of the Company's needs and relevant legal provisions;
- supervise, with the support of the designated figures, compliance with internal regulations and provisions regarding the protection of Personal Data;
- verify and submit to the Board of Directors the annual reports shared by the Data Protection Coordinator and the DPO;
- provide support to other Group companies in carrying out activities within its competence (e.g., directing the design of strategic initiatives in compliance with the principle of privacy by design and by default);
- appropriately store the documentation produced and used in the performance of activities within its competence.

It should be noted that, when necessary, the Data Protection Committee may make use of the Data Protection Coordinator, Support Functions and the DPO as well as additional individuals in order to carry out its duties.

#### 6.2 DATA PROTECTION COORDINATOR

The Data Protection Coordinator, provided only within the organizational structure of the Company, coordinates the Data Protection Referents who play a key role in the protection of Personal Data and consults, when necessary, with the DPO to perform the following tasks:

- keep abreast of new changes or regulatory interventions, measures or practices, guidelines or opinions on Data Protection;
- build / update, with Support Functions and Data Protection Referents, internal provisions on Personal Data Protection, submitting them, as appropriate, for the attention of the Data Protection Committee and the DPO in the light of, inter alia, regulations and practices on Personal Data Protection and corporate and organizational events;
- assisting the People Department in the design and delivery of staff awareness and training activities regarding regulatory obligations and internal provisions on Personal Data Protection;
- keep up-to-date, with the support of the Data Protection Referents and supporting Functions, the record
  of processing activities carried out by the Company ("Record"), both as Data Controller and as Data
  Processor;
- propose to the Data Protection Committee and/or the Data Protection Referents any changes to the internal provisions on the protection of Personal Data, as well as to the general and specific instructions on processing, which may result in benefits related to recovering efficiency or increasing the effectiveness of the Model; analyze, manage and keep track, with the support of the DPO and the relevant functions, of the following events: design of new initiatives; analysis and mitigation of risks associated with processing; data protection impact assessments and prior consultation; selection and appointment of data processors pursuant to Art. 28 of the GDPR; transmissions of Personal Data to third parties; transfers of Personal Data to third countries or international organizations; management of requests to exercise data subjects' rights; management of security incidents and breaches of Personal Data;
- serve as a point of contact for:
  - Delegate of Data Controller and the Data Protection Committee, regarding the Company's level of compliance and risks in relation to its obligations under Personal Data protection regulations and practices;
  - Data Protection Referents, regarding regulatory obligations and internal provisions on Personal Data Protection and events to be handled (e.g., new initiatives, Personal Data breaches etc...);
  - the DPO, on all relevant Personal Data protection issues and events to be handled for which a DPO opinion is required (e.g., new initiatives, Personal Data breaches);
- collaborate with the DPO and the corporate functions in charge within the scope of the audits carried
  out by them and implement the appropriate corrective actions aimed at remedying the reported noncompliances;

- provide, if requested by the Data Controller or its Delegate, support in the event of any complaints, judicial and extrajudicial disputes regarding data protection;
- prepare an annual report regarding the activities carried out during the past year and the activities planned for the new year to ensure adequate protection of Personal Data, also in light of the results emerging from the risk assessment activity;
- receive and analyze reports periodically submitted by:
  - DPO, as part of the audits carried out periodically and in the manner defined by the service contract;
  - Data Protection Referents as part of the audits carried out periodically and in the manner defined by the audit program;
- provide support to other Group companies in the management of compliance required by regulations and practices regarding the protection of Personal Data;
- involve the Data Protection Referents on matters requiring his/her involvement, with particular reference to those involving the exercise of spending powers attributed to the Data Protection Referent;
- process and appropriately preserve the documentation produced and used in the performance of the activities within its competence.

#### 6.3 DATA PROTECTION REFERENTS

Data Protection Referents are corporate individuals (Functional Directors) who work under the authority of the Data Controller and who are assigned by the latter, under their own responsibility, specific tasks and functions related to the processing of Personal Data within the Department they head. The Data Protection Referents in compliance with the requirements of the GDPR, other Union or Member State provisions relating to data protection as well as the processes and rules defined by the Data Protection Coordinator and limited to the processing under their responsibility, shall:

- with the support of the Data Protection Coordinator and supporting Functions, update the internal provisions on Personal Data protection, and keep up-to-date the record of processing activities, both as the Data Controller and the Data Processor;
- prepare and share with the DPO, the Data Protection Coordinator and the relevant Data Protection Referents, communications to be sent externally on behalf of the Data Controller, with particular regard to notifications/communications to be sent to the Supervisory Authority and data subjects, also ensuring that the communication is actually sent;
- define and implement, with the support of the Data Protection Coordinator, Support Functions and relevant Data Protection Referents, technical and organizational measures aimed at ensuring compliance with the principles of Personal Data protection by design and by default set forth in Article 25 of the GDPR;
- carry out analysis and verification regarding the likelihood and severity of risks to the rights and freedoms of data subjects associated with processing, including in the event of a data breach;
- verify the implementation of and compliance with the internal provisions for the protection of Personal Data, as well as with the general and specific instructions on the specific processing or with the provisions indicated with respect to third party recipients (such as autonomous data controllers, Data Processor ex art. 28 of the GDPR or Authorized Persons of the processing);
- prepare, on the basis of the instructions received from the DPO, an appropriate attestation/reporting to be transmitted to the DPO and/or to the Data Protection Coordinator on a periodic basis regarding the compliances managed by its delegates and, on the latter's instructions, by the Authorized within its area of competence, including critical aspects to be managed;
- collaborate with the DPO and/or the designated corporate functions within the scope of the audits carried out by them and implement the appropriate corrective actions aimed at remedying reported noncompliances;
- process and appropriately preserve the documentation produced and used in the performance of the activities within its competence.

In the event that the Data Protection Referent in charge of a Function does not have Internal Referent within his or her structure, the tasks referred to in the appointment as Internal Referent, fully reproduced in the present appointment, shall be understood to be the responsibility of the Data Protection Referent.

#### 6.4 DATA PROTECTION OFFICER

The Data Protection Officer is a figure provided for in certain cases regulated by Article 37 paragraph 1, of the GDPR on a mandatory basis. It is a person designated by the Data Controller or Data Processor to perform support and control, advisory, training and information functions with regard to the application of the regulation itself.

#### The DPO is responsible for:

- oversee compliance with the Regulation, other Union or Member State provisions relating to data protection
  as well as the Data Controller's (Controller) or Data Processor's (Processor) policies on the protection of
  Personal Data including the allocation of responsibilities, awareness raising and training of staff involved in
  processing and related control activities (Art. 39 GDPR; 4.1 Guide-Lines on DPOs, April 5, 2017);
- cooperate with and act as a point of contact for the supervisory authority on matters related to the processing of Personal Data, including prior consultation, and carry out consultations regarding any other matters as appropriate (Art. 39 GDPR; 4.3 Guide-Lines on DPOs, April 5, 2017);
- informing and advising the Data Controller (Controller) or Data Processor (Processor) as well as employees
  who process Personal Data about their obligations under the GDPR as well as other Union or Member
  State provisions relating to data protection (Art. 39 GDPR);
- provide advice, if requested, on the data protection impact assessment (DPIA) and oversee its conduct (Art. 39 GDPR; 4.2 Guidelines on DPOs, April 5, 2017). The Working Party recommends that the Data Controller consult with the DPO on the following issues, among others:
  - whether or not to conduct a DPIA;
  - what methodology to adopt in conducting a DPIA;
  - whether to conduct the DPIA with internal resources or by outsourcing it;
  - what safeguards to apply, including technical and organizational measures, to mitigate risks to the rights and interests of data subjects;
  - whether or not the DPIA was properly conducted, and whether or not the conclusions reached (whether
    or not to proceed with processing, and what safeguards to apply) are in accordance with the GDPR.

If the Data Controller does not agree with the guidance provided by the DPO, the DPIA documentation must specifically state in writing the reasons for not complying with the guidance.

- develop and keep up-to-date a record of processing activities carried out by the Company to be shared, where required, with the Supervisory Authorities (4.5 Guidelines on DPOs, April 5, 2017);
- duly consider the risks inherent in the processing, taking into account the nature, scope, context and purposes of the processing, focusing on the highest risk areas (Art. 39 GDPR; 4.4 Guidelines on DPOs, April 5, 2017). In essence, the DPO is asked to prioritize his or her work and focus on those issues that present the highest data protection risks. While this does not mean that the DPO should neglect to monitor the degree of compliance of other processing associated with a comparatively lower level of risk, in fact the provision signals the desirability of giving priority attention to areas that present higher risks. Through this selective and pragmatic approach, the DPO should be more easily able to advise the Controller which methodology to follow in conducting a DPIA, which areas to reserve an internal or external data protection audit for, which internal training activities to provide for staff or administrators who process Personal Data, and which processing to devote more resources and time to.

The Data Protection Officer, who serves in this role for D-Orbit S.p.A., has been contracted to a third party company in compliance with the requirements set forth in the GDPR and former WP29 ("Guidelines on Data Protection Officers").

#### 6.5 SUBJECTS AUTHORIZED TO PROCESS

The Subjects Authorized to Process are all employees who carry out Personal Data processing operations necessary for the performance of the tasks entrusted to them, pursuant to Articles 29, 28 par.3(b) and 4(10) of the GDPR and Article 2-quaterdecies of the Privacy Code, and who operate under the direct control of their Data Protection Referent. The Subjects Authorized to Process<sup>2</sup> in compliance with the requirements of the GDPR, other Union or Member State provisions relating to data protection as well as the company's internal provisions, and **limited to the processing within their competence**, must:

- carefully guard the authentication credentials that have been provided to them to allow access to the
  company premises and systems containing the Personal Data subject to their processing and the company
  tools provided by the Data Controller for the exercise of their duties (e.g.: personal computer, company cell
  phone, badges, keys, passwords) and manage any loss or theft of them promptly informing their dp in
  accordance with company procedures;
- collect, manage and store processed Personal Data in such a way as to ensure compliance with the
  principles of integrity, confidentiality, availability of data, minimization of processing and limitation of
  storage, as well as to minimize the risks, including accidental, of unauthorized access and processing that
  is not permitted or does not conform to the purposes of data collection, destruction and loss;
- refrain without prior consultation with the Data Controller from creating new and autonomous databases, with purposes other than those already envisaged at the company level;
- not disclose or communicate to third parties the Personal Data of which it becomes aware and which is the subject of its own processing, outside the cases permitted by law and/or company procedures;
- not leave the computer workstation unattended in any way by allowing accessibility to the data; by way
  of example only, do not leave authentication credentials unattended on the computer screen or computer
  workstation, store all magnetic media used in the archives; media no longer used may only be deleted or
  destroyed after the Personal Data contained therein has been rendered effectively unusable;
- carry out, based on the instructions of the Delegated Data Protection Referent, the following activities where applicable to the relevant processing operations:
  - collect Personal Data directly from the data subject from the processing or from third-party sources;
  - give information to data subjects from the processing pursuant to Articles 13 and 14 of the GDPR and collect consents for the processing of Personal Data;
  - historicize the consents given by the data subject, the date on which they were given and, if revoked, the
    date on which such revocation occurred;
  - highlight in a timely manner to the Delegated Data Protection Referent and/or the Data Protection Coordinator any changes to be considered to be made to the processing carried out within their Office of belonging;
  - process, in compliance with the applicable principles and the conditions of lawfulness of the Processing, the Personal Data related to the processing of its area of competence as resulting from the record of processing activities;
  - retain Personal Data in compliance with company regulations/for a period of time not exceeding the
    achievement of the purposes for which they are collected and processed. Such retention shall in no case
    exceed the retention period stipulated in the record of processing activities for each processing activity
    carried out by its Office;
- provide support, where involved by the Delegated Data Protection Referent, in carrying out the analysis of risks to the rights and freedoms of data subjects and in defining appropriate technical and organizational measures;
- provide support, where involved by the Delegated Data Protection Referent, in carrying out the Personal Data Protection Impact Assessment (DPIA) and possible prior consultation to the Supervisory Authority;
- act in compliance with the rules of conduct and secure use of IT resources and services, with particular reference to resources and services involving the processing of Personal Data;

<sup>&</sup>lt;sup>2</sup>In the event that the Subject Authorized to process does not hierarchically have an Internal Referent above him/her, he/she will report directly for the performance of his/her duties to his/her Data Protection Referent.

- comply with the procedures and, in particular, the instructions that have been given to them by this deed and/or subsequent supplementary acts authorizing them to process only the Personal Data subject to their own processing reported in the record of processing activities, within the limits of the tasks and duties entrusted to them;
- provide support to the functions in charge in the execution of controls aimed at verifying the level of compliance regarding the protection of Personal Data;
- appropriately preserve the documentation produced and used in the performance of the activities within their competence.

#### 6.6 SYSTEM ADMINISTRATORS

The professional figure envisaged for Italian companies by the Provision of the Italian Data Protection Authority of 27.11.2008 published in Official Gazette of the Italian Republic no. 300 of 24.12.2008, who, in the IT field, maintains, configures and manages (i) a data processing system or its components, including complex software systems such as Enterprise Resource Planning systems (system administrator), or (ii) a database (database administrator), or (iii) networks and telecommunications security equipment (network administrator) is appointed System Administrator.

The assignment of the functions of System Administrator is made after assessing the characteristics of experience, capacity and reliability of the designated person, who provides suitable guarantees of full compliance with the current provisions on Processing, including the profile relating to security.

In this regard, individuals possessing the following requirements may be identified as System Administrators:

- competence in the IT field, also in relation to issues related to the security profile, for example in view of the educational background and/or professional experience gained;
- compliance with regulatory and corporate provisions on the Processing of Personal Data;
- after consultation with the Data Protection Referent, the System Administrator is identified and appointed by the Delegate of the Controller, after consulting the People and IT Functions.

#### 6.7 OTHER PLAYERS INVOLVED

#### 6.7.1 Data Processors

Processors are third parties (e.g., suppliers, consultants, dealers, agents) who carry out one or more processing activities on behalf of D-ORBIT in accordance with Article 28 of the GDPR, providing sufficient guarantees to put in place appropriate technical and organizational measures so that the processing meets the requirements of the GDPR and ensures the protection of the rights of the data subject.

#### 6.7.2 Data Subjects

Data subjects are the individuals to whom the Personal Data refers (e.g., employees, candidates, prospects and customers, visitors). Data Subjects give their explicit consent to the processing of such Personal Data for one or more specific purposes and have the opportunity to make requests to the Data Controller or Data Processor to exercise their rights (to revoke their consent at any time; to obtain confirmation as to whether or not Personal Data concerning them is being processed and if so, to obtain access to the Personal Data; etc.).

#### 6.7.3 Supervisory Authority

The Supervisory Authority is competent to perform the assigned tasks and exercise the powers conferred on it under the GDPR in the territory of the respective Member State. If the processing is carried out by public authorities or private bodies acting on the basis of Article 6 (1) (c) or (e), the Supervisory Authority of the respective Member State is competent. In that case, Article 56 shall not apply. Supervisory authorities shall not be competent to supervise processing carried out by courts in the exercise of their judicial functions.

# **7** ANNEXES

ID	Item	Object
1	Model of approval of the Organizational Model	
2	Model of Appointment of Data Protection Coordinator	
3	Model of Appointment of Data Protection Referent	
5	Model of Appointment of DPO	
6	Model of Appointment of Subject Authorized	
7	Model of Appointment of System Administrator	
8	Mode of Appointment of Data Processor	

