# POLICY

# doValue Group
# Data Protection

# INDEX

# 1 GENERAL INFORMATION ABOUT THE DOCUMENT

| | |
|---|---|
| **Issuer Company** | doValue S.p.A. |
| **Target Company/ies** | All doValue Group companies (Parent Company and Subsidiaries in Italy and abroad) |
| **Title** | doValue Group Data Protection |
| **Issue date** | 13/01/2021 |
| **Effective date** | Immediately |
| **Document identification code** | PL02-2021-R01 |
| **Hierarchical level of Integrated Regulatory System** | III Hierarchical Level |
| **Document Type** | Policy |
| **Regulatory directive** | Yes |
| **Prepared by (Owner):** | Compliance & Global DPO |
| **Reviewed by:** | General Counsel |
| **Approved by (Accountable) on:** | Board of Directors of doValue on 17/12/2020 |
| **Issued via:** | Service communication no. PL02-2021-R01 |
| **Documents rescinded or replaced:** | III-Policy R&C-11-2018-R02 - Policy in materia di protezione dei dati personali |
| **Timeline of revisions** | R01 – First Version |

## 2 GLOSSARY

| | |
|---|---|
| **Supervisory Authority (or Authority)** | The Authority described in Article 51 of the GDPR ("General Data Protection Regulation") i.e., one or more independent public authorities appointed by a Member State to be responsible for monitoring the application of the Regulation, in order to protect the fundamental rights and freedoms of natural persons in relation to personal data processing. |
| **Subsidiaries** | The financial and/or ancillary companies included in the doValue Group. |
| **Judicial data** | Personal data that may reveal the existence of specific judicial proceedings subject to inclusion in a criminal record (e.g. definitive criminal convictions, conditional release, residence ban or obligation, alternative non-custodial measures) or the status of accused person or person under investigation. |
| **Personal data** | Any information relating to an identified or identifiable natural person ('Data Subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. |
| **Identification data** | Identification data are data wherefrom it is possible directly to identify the Data Subject.<br>For example, identification codes including those forming part of personal details (e.g. tax number) and unique codes assigned to a person based on predefined criteria (e.g. customer codes) are identification data. |
| **Sensitive data** | Personal data capable of revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. |
| **Banking data** | Personal data regarding the banking or financial relations of the Data Subject and related instructions (e.g. payment instructions). |

| | |
|---|---|
| **Data Protection Officer (o "DPO")** | The "Data Protection Officer" is the person designated by the Controller (or Processor) to carry out support and control, consultation, training and information functions in relation to application of the GDPR. |
| **General Data Protection Regulation (or "GDPR")** | The "General Data Protection Regulation" i.e., Regulation (EU) no 679 of 27 April 2016 which establishes the European system of regulation on the protection of natural persons with regard to the processing of personal data and the free circulation thereof. |
| **Group** | The doValue Group, including doValue (Parent), Italfondiario, doData and foreign subsidiaries for Region Iberia and Region Greece and Cyprus. |
| **(Data) Subject** | A natural person identified or identifiable, directly or indirectly, by a piece of personal data and, in any case, to whom the processed data refers. |
| **Principal** | The bank, SPV or other legal person that gives a do Value Group Company a mandate for credit recovery activities and/or related and ancillary services. |
| **(Data) Processor** | A third party other than an employee or a legal representative that is appointed as Processor in relation to personal data processing carried out by it on behalf of the Controller by means of a service or collaboration agreement that specifies the scope of the delegated responsibilities. |
| **Data Controller** | The natural or legal person, Public Authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. |
| **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. |
| **Company(ies)** | One or more companies of the doValue Group |

# 3 INTRODUCTION

In a constantly evolving, interconnected global environment, it is essential to pay the necessary attention to Personal Data protection in light of the new vulnerabilities and threats that lead to increased risks in relation to the processing of Personal Data and require ever more careful management of all phases of the processing process from collection to disposal of the data.

The scope of this Policy is to set out:

- The **Data Protection strategy of the doValue Group**, outlining the Group's commitment to personal data protection.
- the **Organisation Model for Personal Data Protection** (hereinafter, also "**OMPDP"**), which describes the roles, responsibilities and inter-relations between the various figures identified for the governance of the personal data management system of the Group companies.
- the **Data Management Model** which outlines the main requirements of the European Regulation for proper governance of Personal Data processing.

## 3.1 APPLICABILITY

This policy applies to all doValue Group companies, in Italy and abroad and it is adopted by means of separate resolutions of the Boards of Directors of the Parent Company and the Italian and non-Italian subsidiaries which, in coordination with the Parent Company, undertake, through their governance body with responsibility for strategic supervision, to implement its principles and guidelines, while taking account of the particular features of their businesses and of the local regulations.
The policy is aimed at all the internal personnel of doValue and the subsidiaries who process personal data.

## 3.2 LEGISLATIVE AND REGULATORY BACKGROUND

The document has been prepared pursuant to the personal data protection regulations, on a European level and on an Italian level, contained in the following, as subsequently amended:

- General Data Protection (EU) 679/2016 (hereinafter "GDPR")
- Guidelines issued by the" Article *29 Data Protection Working Party"* (in short, also, "WP29") and/or the European Data Protection Board (in short, also, "EDPB")
- Legislative Decree No. 196 of 30 June 2003 "Personal Data Protection Code" as amended and supplemented by Legislative Decree No. 101/2018 and other local national regulations applicable to Group Companies.

## 3.3 GENERAL PRINCIPLES

The GDPR lays down the principles relating to processing of personal data, establishing that personal data shall be:

a) processed lawfully, fairly and in a transparent manner in relation to the Data Subject ("**lawfulness, fairness and transparency**");
b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes ("**purpose limitation**");
c) adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed ("**data minimisation**");
d) Accurate and, where necessary, kept up to date; every reasonable step must be adopted to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased, or rectified without delay ("**accuracy**");
e) kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the personal data are processed ("**storage limitation**");
f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical and organisational measures ("**integrity and confidentiality**").

# 4 DATA PROTECTION STRATEGY

The Group's core business involves the management of non-performing loans and receivables on behalf of Principals (e.g. Principals/Banks/SPVs) and all other court and out-of-court activities directly or indirectly related to the core business described above. In this context, the doValue Group companies have to manage:

- several different types of personal data (Identification, Sensitive etc.);
- various categories of Data Subject in relation to which the Group companies may act as Data Controllers (employees, clients, potential clients, third parties, etc) and/or as Data Processors (i.e., the data of obliged parties processed under credit recovery appointments in relation to which the principal Banks are the Data Controllers).

The doValue Group undertakes to guarantee the security and protection of the personal data processed by all of its employees and collaborators, by means of a risk-based approach consistent with the applicable legal and regulatory requirements and all stakeholder expectations (as better defined below).

The doValue Group constantly monitors legal and regulatory developments in the field of personal data protection with the aim of taking appropriate action to ensure that its personal data protection system is constantly updated and improved. Moreover, based on their level of exposure to the risk of a loss of confidentiality, integrity, and availability of personal data, all do Value Group Companies implement appropriate technical and organisational security measures with the aim of reinforcing the protection of the personal data processed, while respecting the principle of accountability.

## 4.1 STAKEHOLDER

The stakeholders in the doValue Group data protection system are those parties that benefit from the proper set-up of the system in accordance with all regulatory requirements applicable to the specific context in relation to personal data protection. Specifically, they include:

- **Investors** as any reputational damage caused by the improper processing of personal data could lead to a reduction in the value of shares and a loss of investor confidence in the organisation;
- **Board of Directors** as the regulatory/legislative compliance of the DP system ensures mitigation of the risk of non-compliance that could lead to the imposition of penalties by the Supervisory Authority with potential financial losses and reputational damage for the Group;
- **Data subjects** as a weak personal data protection system would increase the Group companies' level of exposure to the risk of the loss of confidentiality, integrity and availability of the personal data processed. Therefore, the occurrence of an event that affects the confidentiality, the integrity, and the availability of the personal data of Data Subjects could cause damage to the Data Subject, possibly significant damage.
- **Principals** because, in relation to the services rendered, the doValue Group companies may be designated as Processors operating on behalf of principals that act as Controllers. Consequently, the principals benefit from the strength of the Data

Protection System of the doValue Group companies, and it becomes essential to the protection of personal data in respect of which they are Controllers.

## 4.2 DATA PROTECTION PROGRAMS

A robust personal data protection system is a fundamental requirement for organisations operating in the financial sector. Growing demand for reliability and compliance with specific requirements leads, on the one hand, to a higher level of complexity for cyber risk management and, on the other, to increased client confidence in Group companies.
The programs that compose part of the do Value Group's Data Protection system aim to ensure compliance with European and national data protection legislation minimise the risk of a loss of confidentiality, integrity and availability while protecting the business's information assets which largely consist of personal data. Therefore, the doValue Group undertakes to:

- achieve an integrated, consistent, and harmonious approach to personal data management by establishing the guidelines that have to be followed on a local level by all subsidiaries, in Italy and abroad;
- reduce the risk of data loss through targeted measures for the employees and third parties involved in personal data processing;
- use advanced security tools to detect threats to data security and take effective action to combat such threats;
- take a security by design approach for all new technologies that are adopted by the Group companies.

## 4.3 RESOURCES ALLOCATED

The doValue Group undertakes to guarantee the allocation of adequate resources in operational and financial terms with the objective of monitoring regulatory developments in the field of personal data protection and promptly identifying the action required in order to adapt and update the data management model and personal data processing support tools, also with a view to strengthening security measures.

# 5 THE DATA PROTECTION ORGANISATIONAL MODEL

The data protection organisational model (DPOM) adopted by the doValue Group has been designed on the basis of the business characteristics of the Group companies and on the basis of relations between those companies.
As shown in the following chart (see Fig.1), the DPOM is organised into two areas:

- **Governance & Supervision:** whose duties include: (i) determining the approach of the data protection system, its objectives, and related methods of personal data processing; (ii) ensuring that the organisational complies with the requirements of data protection regulations; (iii) coordinating approved initiatives in the area of data protection; (iv) acting as a focal point on Data Protection issues, playing a consultative and contact role in relation to the Supervisory Authority.

- **Operational Areas:** which are responsible for operational duties and activities in relation to personal data processing, depending on the internal or external role filled (business departments, ICT and third parties)

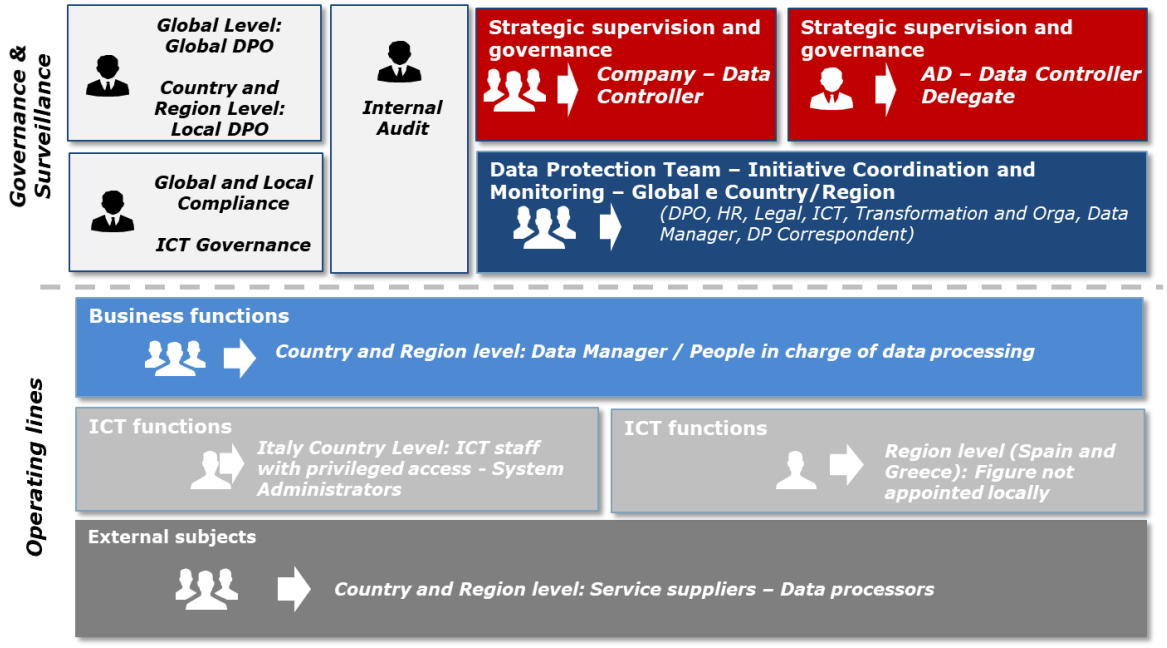



Fig. 1 – doValue Group DPOM

The complexities involved in personal data protection mean that a number of roles, with specific duties and responsibilities in relation to Data management, have to be appointed. Some of these roles are specifically provided for by the GDPR (or by Orders of the Supervisory Authority, where applicable), as follows:

- the Controller
- the Data Protection Officer (DPO)
- the Processor and, where designated, the Sub-Processor
- the System Administrator (where provided for under local regulations).
- the Person in charge of Processing

Other roles are appointed as a result of management decisions, taking account of the organisational structure and processing methods. They help with the proper functioning of Personal Data management safeguards and include:

- the Data Protection team;
- the Data Manager;
- the Personal Data Protection representative.

## 5.1 GOVERNANCE ROLES

The main task of the governance roles is to direct Group activities in order to ensure that the personal data of Data Subjects are protected and that their rights under the regulation are respected.

### 5.1.1 The Controller and the Delegate

Article 4(7) of the GDPR defines the Controller as « *the natural or legal person, Public Authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data* »
Therefore, the Controller is responsible for determining the purposes and means of the processing carried out, adopting organisational and technical measures capable of ensuring compliance with the regulation, reviewing, and updating such measures whenever necessary and guaranteeing Data Subjects the right to exercise their rights recognised by the GDPR. Moreover, it is the duty of the Controller to designate the Data Protection Officer (DPO), asking him or her to supervise the personal data protection system.
Within the Group, each Company, as represented by its Board of Directors, is the Controller for the purposes of the processing of data acquired and managed by it in connection with its operations.
The Board of Directors may designate the Managing Director as "**Controller's Delegate**" in order to fulfil the Controller's regulatory compliance requirements in relation to the relevant Company. In turn, the Controller's Delegate may sub-delegate fulfilment of certain of the Controller's tasks to other individuals within the Company e.g. appointment of Processors, as provided for by the internal rules on sub-delegation currently in force.

### 5.1.2 Data Protection Team

The Data Protection Team is an optional working group, which is given **duties of coordination and strategy** in relation to data protection.
The Data Protection Team is convened depending on specific operational requirements to facilitate collaboration between key players that already have a Data management role in their ordinary activities. For example, the Data Protection Team may be convened in case of a data breach or in case of evaluation of new services/processing in accordance with the principle of Privacy by Design and Privacy by Default.
The Data Protection Team comprises the DPO, the Compliance department the data protection correspondents, who may be joined by representatives of the Human Resources, Transformation and Organisation function, the Legal area, the ICT sector, as well as Data Managers, for issues of their interest
The Data Protection Team fulfils the following requirements:

- Enable the coordination and monitoring of initiatives undertaken by the Controller with an impact on Data Protection;
- Support the DPO with performance of those tasks that require a more detailed insight into the Group's organisational structures;
- Support the DPO with data breach management activities;
- Act as a point of contact and discussion between the DPO and the Data Managers.

### 5.1.3 The Compliance Unit

The compliance unit – where it exists – ensures that the organisation complies with the requirements of applicable Data Protection regulations.
Its main task involves understanding and identifying the scope of the applicable laws and regulations, as well as their possible impact on business processes and procedures. Specifically, the compliance unit constantly guarantees compliance with internal Data Protection regulations, with reference to organisational changes that may lead to the redefinition of the obligations of the individuals involved.
If a high risk of non-compliance is detected, the compliance unit identifies procedures capable of preventing or, at least, mitigating that risk. It can also support the HR function in identifying the content of Data Protection training that are provided to personnel.
In the course of its activities, the compliance unit maintains its functional independence within the corporate structure.
In some of the Group's legal entities (e.g. Italfondiario, a subject supervised by the Bank of Italy) the compliance function can carry out second-level controls on the basis of local regulations applicable to the entity context.

### 5.1.4 ICT Governance Unit

Regarding to the regulatory framework of personal data security and cybersecurity, the ICT governance function, is in charge of all activities related to IT security and business continuity including the definition of IT policies and procedures.
At Global level, Group IT within the COO function ensures:

- The definition of Group IT and Security strategies/policies, aligned with the evolution of the business strategy;
- The design, maintenance, projects monitoring and optimization of the IT architecture;
- The definition and monitoring of an effective methodology for managing the demand, portfolio and implementation of IT systems;
- The definition of guidelines and monitoring of the annual planning of the Business Continuity and Disaster Recovery Plan defined at Group level;
- The definition and monitoring of the group/local IT budget, safeguarding alignment with the Group's strategic decisions;
- Supervision of the Group's technological innovation;
- The management of third-party service providers by monitoring the key objectives of the local IT service level.

At local level, the ICT Functions, in compliance with the guidelines and coordination defined by IT Group and local regulations, guarantee the implementation of activities related to IT security and business continuity, including the definition of local IT policies and procedures, also by interfacing and supervising IT outsourcers[1], if any.

[1] In doValue at local Italian level, the ICT governance function is identified, within the Retained Organization Function, in the structure Design Authority/ Innovation, Security & BCM, in which the role of the ICT Security Manager is included.

## 5.2 SUPERVISORY ROLES

The primary function of the supervisory roles is to monitor compliance with Data Protection regulations and monitor the risk level for the fundamental rights and freedoms of Data Subjects with regard to the processing of personal data carried out by the company.

### 5.2.1 The Data Protection Officer

The GDPR (Articles 37-39) introduced the role of "Data Protection Officer" (in short, "DPO") obliged Controllers and Processors to make an appointment to this role in certain circumstances (the Authority also recommends designation of a DPO even where it is not obligatory).
The functions fulfilled by the DPO include support and control, consultation, training and information in relation to the application of the GDPR and national data protection laws and regulations. He or she cooperates with the Authority and represents the contact point – also for Data Subjects – for personal data processing issues.
The GDPR provides that Controllers and Processors are obliged to designated a DPO if their core business activities involve processing which requires the regular, systematic monitoring of Data Subjects on a large scale or the large scale processing of particular types of personal data, or data relating to criminal convictions and offences; the Privacy Authority has clarified that such entities include, for example, banks, finance companies, commercial information companies, credit recovery companies, etc. The GDPR also provides that a business group may designate a single DPO on condition that said DPO can be easily reached by each Group company.
Finally, the regulation sets out the requirements of the DPO, providing that he or she shall:

- have appropriate knowledge of data protection law and practices, also in terms of technical and organisational measures or measures designed to guarantee data security;
- carry out his or her functions with complete independence and without any conflicts of interests;
- operate as an employee of the Controller or the Processor or under a service contract (where the designated DPO is external to the Company);
- have sufficient autonomy and resources to carry out the duties effectively. Specifically, the Controller shall guarantee the DPO:
    - a structure comprising an adequate number of collaborators providing support with operating activities
    - a budget that may be utilised at the discretion of the DPO for the operating requirements of the structure, including for the implementation of a plan for the continuing training of the DPO and his or her collaborators.

#### *5.2.1.1 The Global DPO*

Following its analysis of the regulation and the accompanying documents issued on a European and Italian level, the doValue Group decided to designate a Global DPO, on a Corporate level, who operates out of the Parent Company (doValue S.p.A.).
As shown in the following chart (Fig. 2), in the doValue Group corporate and organisational structure, the Global DPO forms part of the Compliance & Global DPO Division and reports hierarchically to the General Counsel and functionally to the Board of Directors which represents the Data Controller.

The lines – different in form and colour – indicate the interrelations between the persons/bodies shown in the chart:

- Hierarchical relationship (solid line): the Global DPO reports to the General Counsel of the Parent Company;
- Functional relationship (broken blue line)**:** the Global DPO reports periodically to the Parent Company BoD;

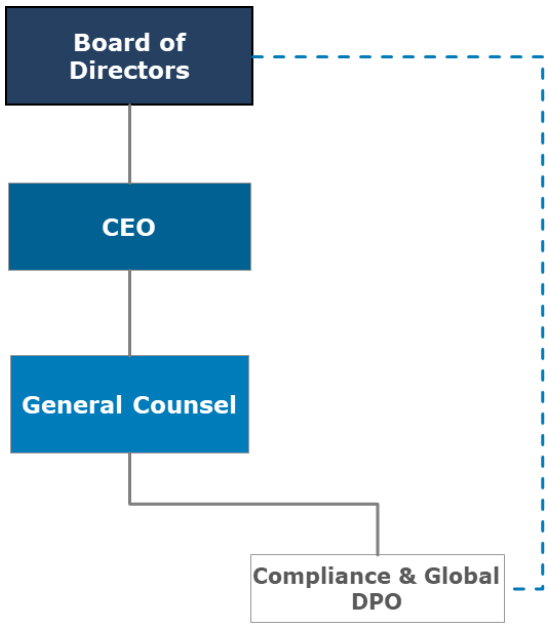



Fig. 2 – Positioning of the Global DPO in the doValue Group

**With reference to the activities of guidance and coordination, the GLOBAL DPO:**

a) defines the Group's Control Framework in the field of Data Protection and the related operational tools for monitoring compliance with Data Protection regulations;

b) receives from all LOCAL DPOs a report on the planning of monitoring activities to be carried out in the coming year (Local DPO Plans);

c) receives from all LOCAL DPOs a report on the results of monitoring activities carried out at Italian and foreign subsidiaries for the purpose of managing risks to the rights and freedoms of data subjects, possible local data breaches or complaints by data subjects that could have a significant impact on the Group, or inspections by local authorities;

d) consolidates the information received and reports to the Board of Directors of the Parent Company a consolidated view at Corporate level on the results of the monitoring activities carried out in the Group, functional to the management of the risk for the rights and freedoms of the Data Subjects, as well as any local data

breaches, complaints and/or privacy requests that could have a relevant impact on the Group;

e) coordinates risk analyses and impact analyses for the rights and freedoms of data subjects connected to cross-sectional project initiatives affecting the Group

f) provides opinions on Data Protection issues affecting the Group or interpretations of data protection regulations applicable to the whole Group

g) supports the definition of personal data protection training plans for the whole Group.

**with regard to surveillance activities related to personal data processing carried out at corporate level, the GLOBAL DPO:**

a) Monitors the data processing activities carried out at Corporate level;
b) Informs and advises the Controller/ Data Manager and the employees who perform the processing about their obligations under the regulation;
c) Supervises compliance with the requirements of the European Regulation and other laws/regulations on personal data protection, as well as compliance with this Policy and internal regulations on personal data protection; this includes the assignment of responsibilities, raising awareness and training personnel involved in processing and related control activities;
d) Provides an opinion in relation to data processing impact assessments performed at Corporate levels in relation to the rights and freedoms of data subjects and oversee performance of any proposed risk reduction action;
e) Cooperates with and act as contact for the Supervisory authority for matters regarding personal data processing performed at corporate level;
f) Act as contact for data subjects for all matters regarding processing of their personal data performed at Corporate level and the exercise of their rights;
g) Prepare internal reports for the Parent Company's governance and control bodies (BoD, CRC, Supervisory Board) on the supervisory activities carried out.

#### *5.2.1.2 Local DPOs*

Local DPOs are appointed by and operate in Italian and non-Italian subsidiaries, and they have following responsibilities:

a) Inform and advise the Controller/ Data Manager and the employees who perform the processing about their obligations under the data protection regulation on a local level;
b) Supervise compliance with the requirements of the European Regulation and other laws/regulations on personal data protection, as well as compliance with this Policy and internal regulations on personal data protection; this includes the assignment of responsibilities, raising awareness and training personnel involved in processing and related control activities. To this end, it prepares an annual plan of control activities

which it submits to the Board of Directors of the Company, after sharing it with the Global DPO (the DPO Local Plan);

c) Provide an opinion in relation to data processing impact assessments performed at Corporate levels in relation to the rights and freedoms of Data Subjects and oversee performance of any proposed risk reduction action. In the case of processing operations which, in the light of an impact assessment, reveal specific risks with regard to the protection of personal data, the LOCAL DPO shall assist the Controller/Processor in consulting the Supervisory Authority with a view to obtaining a prior written opinion from the latter as to whether the processing operation complies with the Regulation;
d) Provide support to HR Unit for training of personnel on Data Protection issues;
e) Cooperate with and act as contact for the Supervisory authority for matters regarding personal data processing performed within the subsidiary;
f) Act as contact for data subjects for all matters regarding processing of their personal data and the exercise of their rights;
g) in the event of personal data breach incidents, pursuant to Article 33 GDPR, the LOCAL DPO shall assist the Data Controller, who must notify the Supervisory Authority of the incident within 72 hours of becoming aware of it;
h) Prepare internal reports for governance and control bodies (BoD, CRC, Supervisory Board) on the supervisory activities carried out in order to manage data protection risks for the rights and freedoms of the data subjects.
i) Prepare an information report for the GLOBAL DPO with the results of monitoring activities performed locally, details or any local data breaches or complaints by data subjects that could have a significant impact on the Group and details of any inspections performed by the Authority;
j) Supervise implementation of Group policies and rules.

Where a doValue Group Company is not obliged to designate a LOCAL DPO (in terms of Art. 37(1)) and a voluntary designation has been excluded, the relevant function shall be guaranteed by the local Compliance or Legal Unit or by another internal structure, whether neither of the said units is present. The following responsibilities shall be assigned to the structure in question:

- oversee compliance with the requirements of the European Regulation and other laws/regulations on Personal Data protection, as well as compliance with this Policy and internal regulations on personal data protection; this includes the assignment of responsibilities, raising awareness and training personnel involved in processing and related control activities;
- provide the Controller with support in handling relations with the Local Authority and/or in handling requests to exercise rights received from data subjects;
- prepare an information report for the Global DPO on any weaknesses identified in the data protection system that that could make the system non-compliant, on any local data breaches or any complaints received from data subjects that could have a significant impact on the Group and on any inspections by the local Authority;
- monitor progress with any activities undertaken to correct any weaknesses identified in the company's personal data protection system.

The charts below show the corporate structure and the relationships between the Global DPO and the Local DPOs of the subsidiaries. The lines – different in form and colour. show the interrelations between the persons/bodies shown in the chart:

- hierarchical relationship (solid line): shows hierarchical relations within the corporate structures
- functional relationship (blue broken line)**:** the Local DPOs report periodically to their respective BoDs
- information and reporting flow (red broken line): Local DPO report to the Global DPO on specific DP issues (i.e. information reports on monitoring activities and management of specific events, coordination of shared activities, inspections by local Authority).

As the following chart (Fig. 3) shows, based on the doValue Group corporate and organisational structure, the doValue Local DPO is situated within the Country Compliance & DPO Division. It reports hierarchically to the Legal Unit and functionally to the Board of Directors which represents the Controller.

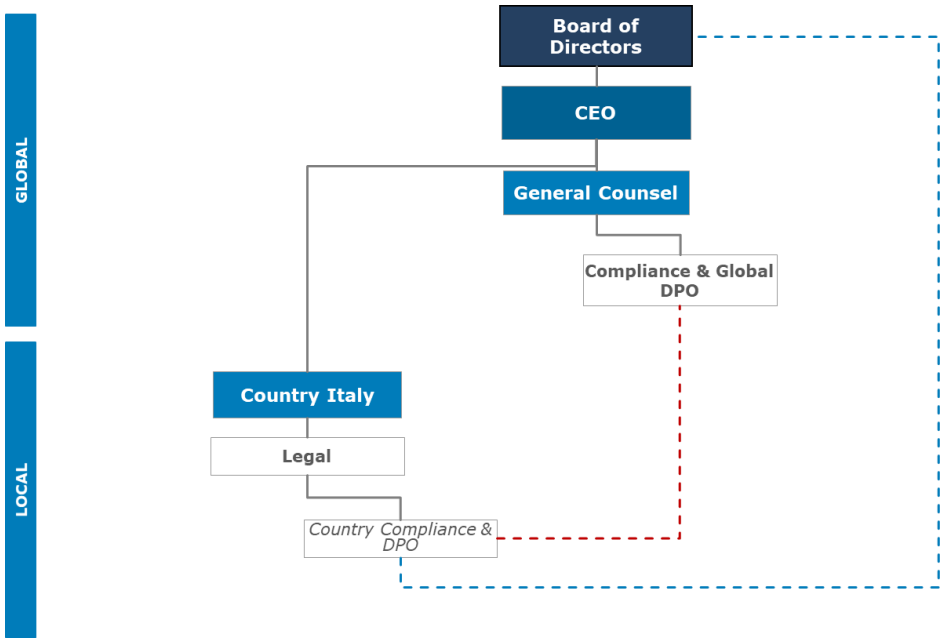



Fig. 3 – Positioning of the Local DPO in the doValue Group

The Local DPOs of Italian Subsidiaries Italfondiario and doData functionally report, respectively, to the Board of Directors and the Sole Director which represent the Controller. Moreover, the Local DPOs have to inform the Parent Company Global DPO about monitoring activities performed locally, local data breaches, and inspections by the Authority or complaints by data subjects.

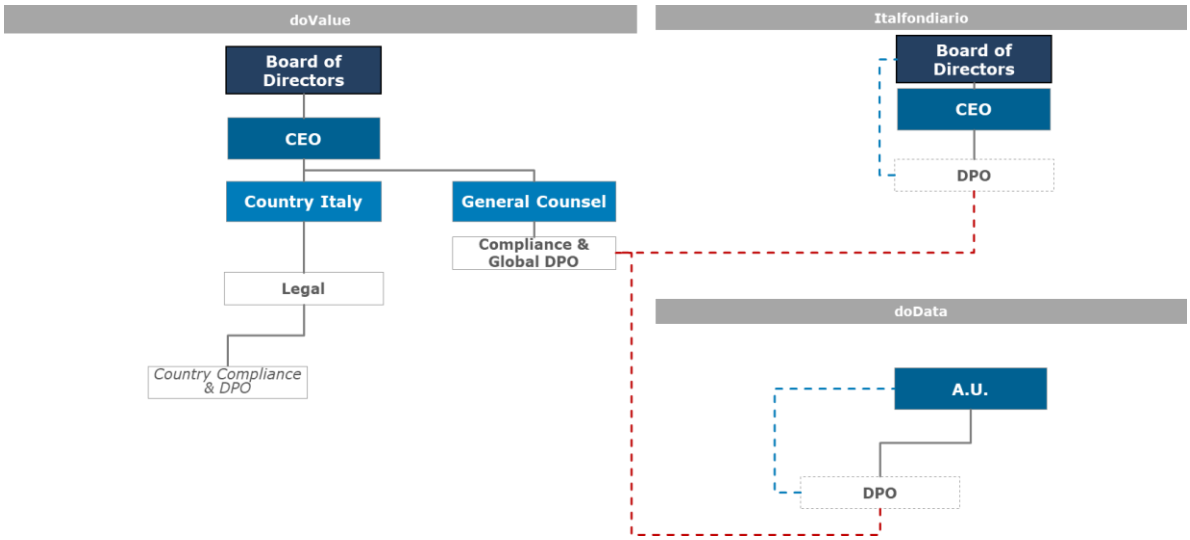



Fig. 4 – Positioning of the Local DPO in the Italian subsidiaries of the doValue Group

The following figures show the relationship between the Global DPO and the Local DPOs of the foreign subsidiaries.

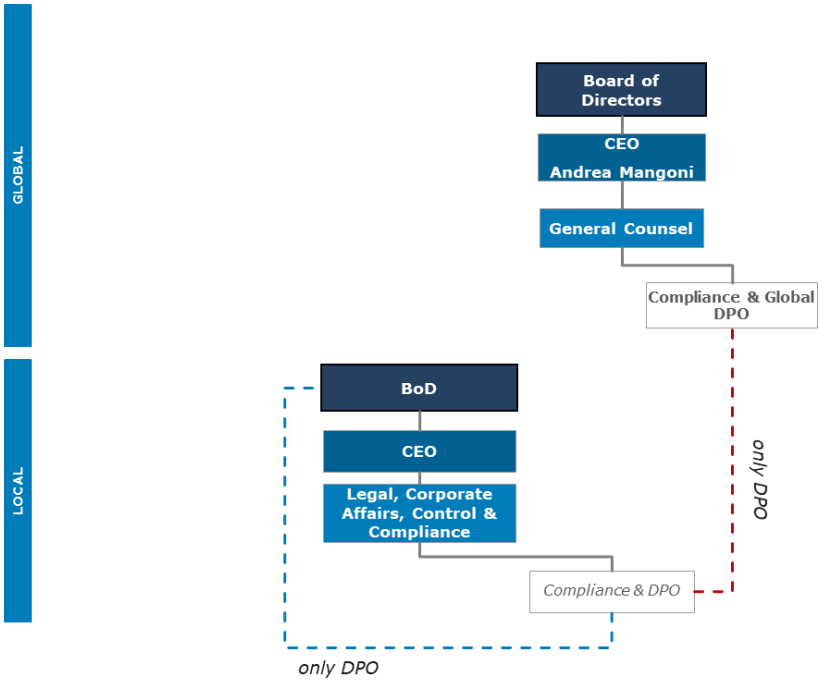



Fig. 5 – Positioning of the Local DPO in subsidiary Altamira

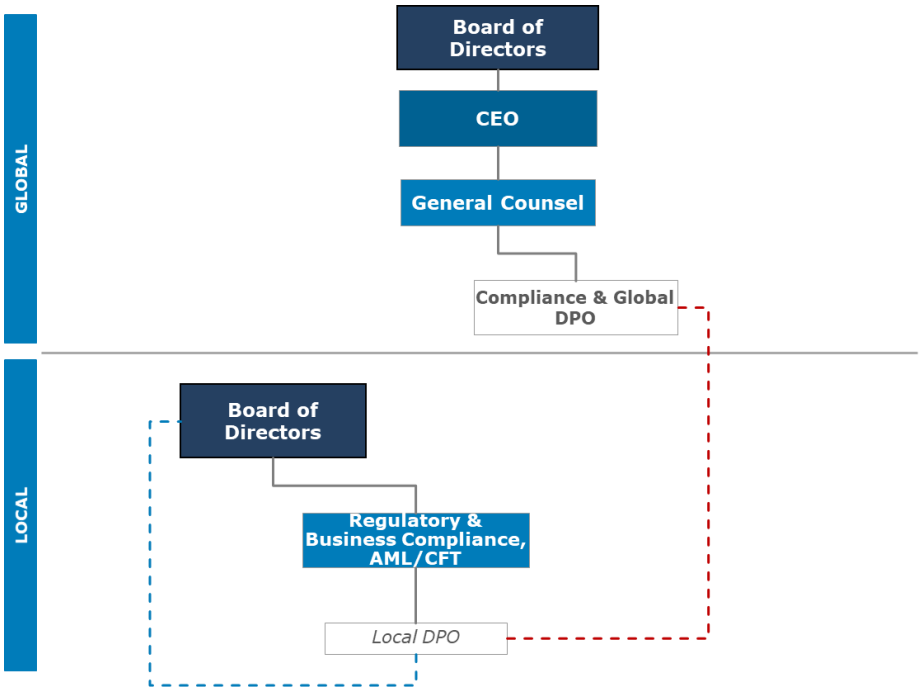



Fig. 6 – Positioning of the Local DPO in subsidiary doValue Greece

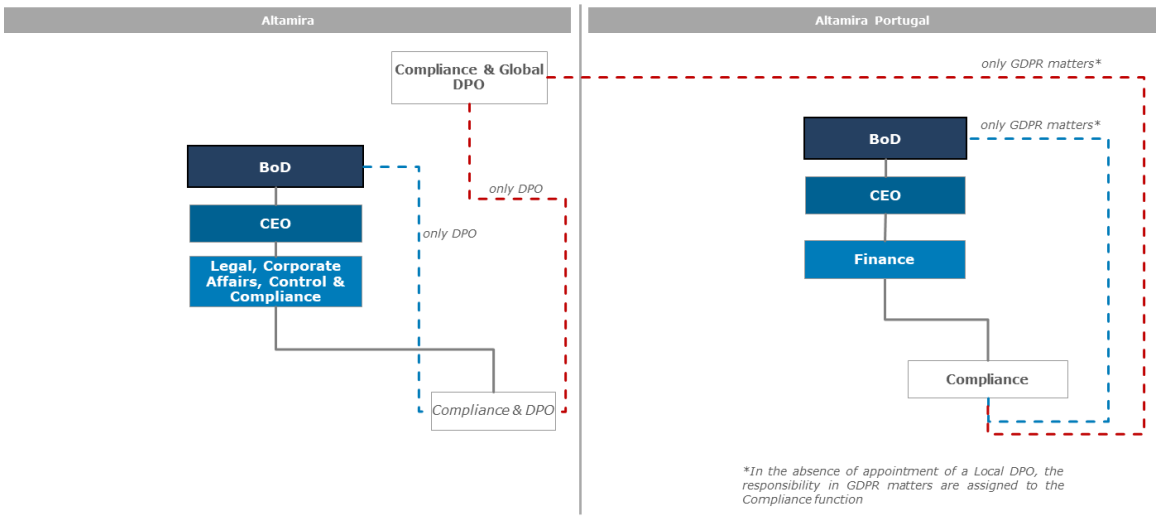



Fig. 7 – Positioning of Local DPO in subsidiaries of Altamira.

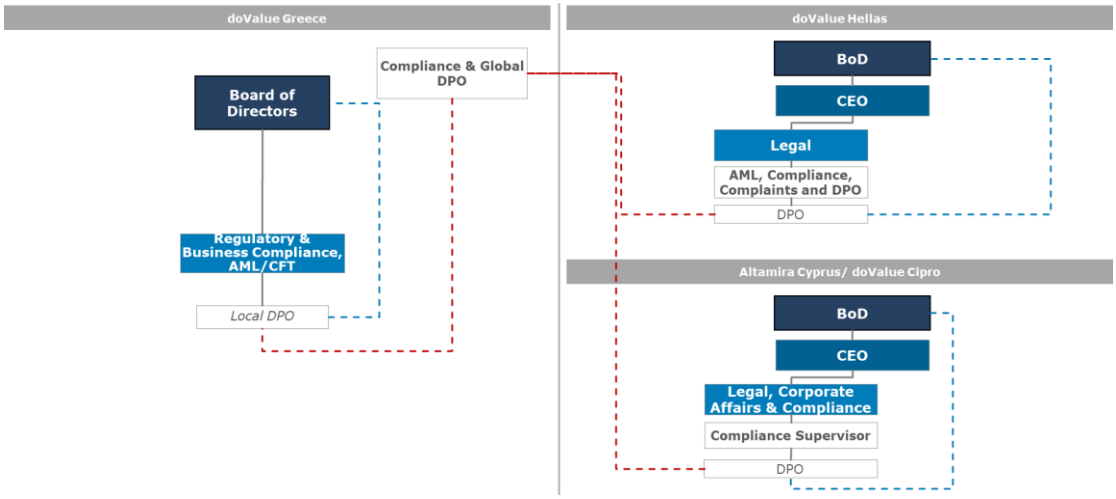



Fig. 8 – Positioning of Local DPO in subsidiaries of doValue Greece.

The contact details of the Local DPOs shall be communicated to the national Supervisory Authority, made known to employees of the Company by means of specific correspondence and communicated to the data subjects.

### 5.2.2 The personal data protection representative

The personal data protection representative is an optional figure supporting the Local DPO with operational management of Data Protection issues. It operates within the company where the role of LOCAL DPO is outsourced to another Group company or to a third-party provider. The personal data protection representative acts as a point of contact with the Local DPO, the Data Protection Team and the Data Managers of individual business departments.
For the subsidiaries, the personal data protection representative is appointed by the Controller's Delegate.
His or her main activities include:

- periodically bringing the Local DPO up to date with data protection issues so that prompt action can be taken if necessary;
- supporting the Local DPO with performance of the activities entrusted to him/her (e.g. monitoring application of requirements of the regulation, management of terms of contract, updating of information notices etc.);
- collaborating with application of the principle of Data Protection by Design and by Default;
- participating in data processing impact assessment in relation to rights and freedoms of Data Subjects
- supporting the creation and updating of records of Processing;
- supporting management of the Data Breach reporting process.

### 5.2.3 The Internal Audit Unit

Independently of the supervisory functions carried out by the DPO, within the framework of the three-year planning cycle defined according to a risk-based logic, the Internal Audit Function (both Local and Group), with a view to level III control, monitors the risks to which the Group is exposed in the processing of personal data of Data Subjects and assesses the adequacy and compliance with the external and internal reference legislation in force at the time, of the control system implemented in the field of personal data protection.
Moreover, upon request and/or authorisation by the Board of Directors, the Internal Audit Unit may assess the adequacy and functionality of the DPO's control framework, reporting such assessments in its periodic reports to the Board of Directors.

## 5.3 OPERATIONAL ROLES

### 5.3.1 Data Manager

Given their supervisory and management role in relation to the activities carried out by the units headed by them and as they have the necessary experience, capability and reliability, Departmental Managers who directly report to the Managing Director or the Board of Directors of Group companies are designated as Data Managers for processing activities relating to their own Department, as documented in the Register of processing activities of the Company to which they belong.
The Data Manager – appointed by means of a specific written document – must check and ensure that all processing carried out by the units under their responsibility are compliant with legal obligations and the requirements of the Authority, as well as with the instructions received from the Controller. They shall also ensure the implementation of the necessary technical and organisational measures to protect the personal data processed; the duties and responsibilities entrusted to them are described in detail in the Data Manager appointment letter, on the basis of the processing carried out in the various units for which they are responsible.

### 5.3.2 Persons in charge of processing

Persons in charge of processing are natural persons who operate under the direct Authority of a Group Company and perform specific tasks and functions connected with Personal Data Processing.
As Controllers, the Companies designate as "Persons in charge of personal data processing" all employees (irrespective of function, grade and/or level) and all collaborators of the Company - irrespective of the contractual relationship (e.g. agency workers, collaborators, trainees, consultants) with the Company – who are issued with authentication credentials for access to the Group's IT network (except for collaborators and consultants working for companies already designated Third Party Processors which, in turn, have to designate the natural persons operating under their Authority as persons in charge of processing).
Each person in charge of processing is required scrupulously to comply with the instructions and security measures set out in their appointment letter, as well as with this Policy and detailed internal regulations.

The content of the instructions is detailed, on behalf of the Controller, by each Data Manager, taking account of the specific Processing activities - and the related means and purposes – carried out in the relevant unit/department and the relevant methods and purposes thereof.

Persons in charge of processing receive training designed to increase their familiarity with the aspects of personal data protection regulations most relevant to their activities, the duties and responsibilities arising and the measures available to prevent harmful events.

### 5.3.3 ICT Unit - System administrators (designated for Italian companies only)

For the Italian Companies belonging to the doValue Group, System Administrators must be formally appointed as provided for in the Order titled *Measures required of controllers who carry out processing using electronic devices in relation to the designation of system administrators* (27 November 2008 as subsequently amended and supplemented).
System Administrators (hereinafter, also "SA") are persons entrusted with the management and maintenance of company information and data processing systems; the term encompasses various roles such as: database administrators, security network and equipment administrators and software system administrators.
In performance of their specialist activities, System Administrators may find themselves carrying out activities that can be considered personal data processing.
The main activities of the System Administrators are to:

- provide Persons in charge of processing and Data Managers with day-to-day support and assistance with technical matters regarding the information systems used for personal data processing;
- report any information system malfunctions to the Data Managers;
- support Data managers (and local DPOs) with analysis of events that have caused data breaches;
- perform maintenance of systems and security protocols.

These activities in foreign subsidiaries, where there is no local requirement to appoint System Administrators, are delegated to the local ICT function.

## 5.4 THIRD PARTIES

Depending on the circumstances and the type of processing, third parties may take on various roles, as described in the paragraphs below.

### 5.4.1 Third parties – Controller

Some third parties may take on the role of autonomous Controller in light of the fact that they provide their services in accordance with professional codes for the sector and/or agency mandates and with assistance from their own organisation. Third parties with the aforementioned characteristics may include: professional advisors (law firms, accountancy firms and notaries).

### 5.4.2 Third parties – Joint Controller

Pursuant to Art. 26 of the GDPR, where two or more controllers jointly determine the purposes and means of processing, they shall be "joint controllers". They shall determine in a transparent manner, based on an internal agreement, their respective responsibilities for compliance with the obligations under the GDPR. doValue Group Companies may assume the role of Joint Controllers in relation to certain data processing carried out jointly.

### 5.4.3 Third parties – Processor

The Processor is a natural or legal person, external to the Company's organisation, which, in the course of contractual relations with Group companies, processes Personal Data in respect of which the Company is Controller.
Pursuant to Article 28.3 of the GDPR, the designation of the Processor and the processing performed by it shall be governed by a contract or other legal act that is binding on the Processor and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of Data Subjects and the obligations and rights of the Controller.
In particular, the Processor shall:

- ensure that Processing activities are legitimate by adhering to the instructions provided, on each occasion, by the Group Company which is the Controller
- ensure that persons authorised to process the personal data have committed themselves to confidentiality
- implement a process for responding to a Data subject seeking to exercise its rights, where the Controller has delegated this function to the third-party Processor or of requests received are immediately transferred to the Controller so that the necessary response can be provided in compliance with the applicable deadline
- provide all of the information necessary to demonstrate compliance with the applicable regulation and the instructions received without affecting the Controller's right to verify proper application of the regulation and compliance with instructions provided
- immediately interrupt Personal Data Processing activities and delete them or make them available to the Controller if the Third-Party Processor is removed from that role or on request by the Controller
- allow any Audits by the Group Companies and provide full collaboration with the detection of any Data Breaches in order to implement the applicable regulatory requirements.

Within the framework of the outsourcing agreements of the activities carried out at corporate level, each Company supplying intra-group services is appointed Manager or Sub-Manager (pursuant to paragraph 5.4.4 below) of the Processing by the other Companies of the Group. Moreover, suppliers and third parties that process data in respect of which Group Companies are Controllers are also so designated as Processor e.g. parties involved in performance of activities related to the products and services offered and in marketing activities for Data Subjects.

### 5.4.4 Third parties – Sub-processor

With the general or specific written authorisation of the Controller, the Third-Party Processor may, in turn, designate another Processor ("the Sub-Processor") with reference to third parties – natural or legal persons – that process personal data in the course of the activities in respect of which it is designated as Processor.
The relationship between the Processor and the Sub-Processor shall, in a manner similar to the relationship between the Processor and the Controller, be governed by a contract or other legal act that specifies duties and responsibilities in terms of Article 28.4 of the GDPR. The Processor accepts full responsibility towards the Controller for the Sub-Processor's compliance with its obligations.
As previously stated, in relation to the Personal Data of obliged entities, as processed in connection with credit recovery activities, the doValue Group Companies operate as Third-Party Processors designated by the Principals in their capacity as Processors. With authorisation from the Controller (general or specific), the Company may use sub-contractors and designate as sub-Processors those suppliers and, generally, those third parties which, under a contract with the companies, process the Personal Data of obliged entities e.g. Third-Party Professional Advisors, Credit Recovery Firms and/or providers of IT services.

## 5.5 RELATIONSHIPS BETWEEN GOVERNANCE AND SUPERVISORY ROLES

The following tables show the relations between the various data protection roles identified by the doValue Group. They specify whether the relationships are based on:

- hierarchical reporting;
- functional reporting;
- information flow and coordination between parties pertaining to various legal entities in the Group
- internal information flow between parties pertaining to the same legal entity;
- Interact with non-Group third parties.

| Functions involved | Relationship | Description |
|---|---|---|
| **Controller – Global/Local DPO** | Functional reporting | • The Controller involves the GLOBAL DPO or the Local DPO in case of an inspection and/or requests by the Supervisory Bodies/Authority at a Corporate or a Local level, respectively.<br>• The GLOBAL DPO prepares a regular report on the supervisory activities performed at a Corporate level, oversees the action necessary to satisfy requests received from the Supervisory Authority and reports to the Controller on the status of action taken at a Corporate level.<br>• The Local DPO prepares a regular report on the supervisory activities performed at a local level, oversees the action necessary to satisfy requests received from the Supervisory Authority and reports to the Controller on the status of action taken at a local level. |
| **GLOBAL DPO – Group IT** | Internal Information Flow | The Global DPO and the Group IT function interface to request opinions on Data Protection issues in the context of the evolution and maintenance of the personal data management system at Group level (e.g. in the case of major IT projects with an impact on the way personal data is managed and protected). |
| **Local DPO – Compliance Unit (if any) + Local ICT Governance** | Internal Information Flow | The Compliance function (if any) and ICT Governance Function interface with the Local DPO in order to request feedback on Data Protection issues as part of the personal data management system maintenance activities |

| Functions involved | Relationship | Description |
|---|---|---|
| **Global DPO- Local DPO** | Information flow and coordination | Subject to the limits set out in Art. 37-39 of the GDPR and while respecting professional independence requirements, the Local DPOs interact with the Global DPO to:<br>• Discuss doubts over the interpretation of the Data Protection regulation<br>• Inform about local events that could trigger risks for the Group personal data protection system (e.g. data breaches, failure to apply principles set out by the GDPR, risk analysis/impact assessment, proper identification of legal basis for processing)<br>• Inform about supervisory activities performed at a local level and reported to the BoD of the Subsidiary<br>• Coordinate monitoring activities to be performed locally<br>• Evaluate the adoption of operational policies/procedures/instructions designed at a local level and/or specific personnel training and awareness sessions on data protection issues. |
| **Local DPO – Data Protection Correspondent** | Functional reporting | For Subsidiaries that outsource the DPO function to the Parent Company Local DPO or to non-Group third parties:<br>• The parent company Local DPO interacts with the Personal data protection representative on all matters relating to personal data processing and on data protection issues regarding the subsidiary<br>• After consulting the Local DPO, the Personal data protection representative issues policies and guidelines and acts as a reference point for business strategy and improvements that prove necessary to the corporate DP system.<br>• The Personal data protection representative interacts and deals with the Local DPO on specific matters regarding organisational and/or regulatory analysis; if any anomalies or issues are identified, they are duly reported to the Local DPO. |

| Functions involved | Relationship | Description |
|---|---|---|
| **Internal Audit – GLOBAL/LOCAL DPO** | Internal Information Flow | Internal Audit interfaces with the Global DPO and the LOCAL DPO to coordinate and receive information on relevant events e.g. data breaches. In addition, the Global and LOCAL DPOs inform the Internal Audit function in relation to the annual plans for surveillance activities and the results of monitoring activities carried out. |
| **Compliance Unit + Local ICT Governance – Data Managers** | Internal information flow | The Compliance Unit interacts with the Data Managers for all matters involved in ensuring the data protection system remains compliant with the requirements of European and local data protection regulations (e.g. updating of register of processing activities, performance of DPIA, drafting of operating instructions)<br><br>The Local ICT Governance function interfaces with Data Managers for all issues related to the maintenance of information systems and related technical security measures in place to protect the processing of personal data. |
| **Global/Local DPOs – Third party processors** | Interaction with third parties | The GLOBAL DPO and the Local DPO (in the Corporate and Local processing environments, respectively) interact with third parties which, pursuant to Art.28.3 of the GDPR, have been designated as Third party processors for all matters which, within the scope of activities assigned by contract, may have an organisational and/or regulatory effect on personal data processing (e.g. reporting of date breaches, scheduled inspections/audits, impact assessments, communications to be sent to the Supervisory Authority) |
| **Local DPO – Data Managers** | Internal information flow | The Data Manager interacts with the Local DPO for requests for opinions in the area of Data Protection during performance of its activities that contribute towards the maintenance of the company data protection system (e.g. updating register of processing activities, performance of DPIA). The Local DPO interacts with the Data Manager for information requests regarding means of processing, the data processed, and any processing problems identified. |

## 5.6 RELATIONSHIPS BETWEEN OPERATIONAL ROLES

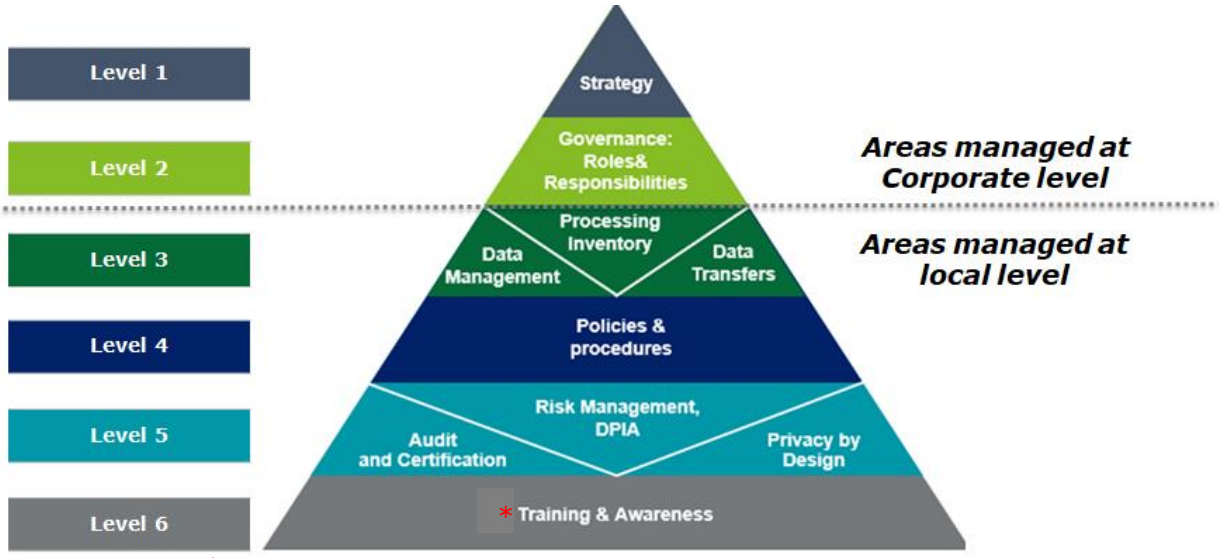
| Functions involved | Relationship | Description |
|---|---|---|
| **Data Managers- Persons in charge of processing** | Hierarchical reporting | Depending on the circumstances, the Data Manager interacts with persons in charge of processing in case of:<br>• instructions/guidelines about means of processing, personal data protection<br>• issues regarding the proper application of security measures introduced to protect the relevant processing<br>• periodical reviews of log of data processing activities<br>• performance of risk analysis and DPIA activities |
| **Data Managers – System Administrators (internal)** | Internal information flow | Depending on the circumstances, the Data Manager interacts with the System Administrators in case of:<br>• instructions/guidelines about means of processing, personal data protection<br>• consequences resulting from IT network/systems malfunction<br>• issues regarding the proper application of security measures introduced to protect the relevant processing<br>• periodical reviews of log of data processing activities in relation to information systems used and security measures implemented.<br>• performance of risk analysis and DPIA activities |
| **Data Managers – Third party processors** | Interaction with third parties | For processing for which he or she is responsible, the Data Manager interacts with the Processors in case of:<br>• instructions/guidelines about means of processing, personal data protection<br>• Requests for specific information needed for performance of the DPIA (e.g. security measures adopted)<br>• Acceptance of reports of Data Breaches<br>• Management of Data Breaches (i.e. gathering of information useful for data breach notification purposes) |

# 6 THE DATA PROTECTION DOCUMENT MODEL

**doValue** has created its own **Data Protection Document Model,** applicable to the **Parent Company** and all of the Group's **subsidiaries** (in Italy and abroad). It consists of a body of documents including:

- at **Corporate** level:
  - high level Group Policy outlining Group DP strategy, the DP organisational model and general DP requirements applicable to all Group companies (as represented by this document);
  - DPO control framework;
  - DPO regulation.
- at **company** level:
  - Operating procedures/instructions for the management of specific matters e.g. data breach management, updating of the Register of Processing Activities, dealing with requests by data subjects etc.
  - Tools/templates prepared in order to comply with specific regulatory requirements e.g. records of personal data processing, registers of data breaches, registers of complaints by Data Subjects, DP designations, privacy information notices, contractual clauses, DPIAs etc.
  - Specific documents prepared to demonstrate performance of specific activities e.g. impact analyses performed on new data processing activities (privacy screening and DPIA), delivery of training sessions on personal data protection issues etc.
  - Specific DPO control framework for corporate context and related reporting.

The Data Protection documentation consists of **6 levels,** each of which has been developed in accordance with international security standards and best practice on Data Protection, as shown in the following diagram. The first two levels refer to issues handled at a Corporate level while the subsequent levels refer to matters handled at a local level by all Group Companies.




* Training & Awareness plans are also defined at corporate level.

Fig.9 – DP Document Model

The following table contains, for each documentation level, a description of the contents that must be included in each component item of the DP documentation.

| Level | Description |
|---|---|
| **Level 1 Strategy** | The Company determines the high-level approach and its risk appetite, on which to develop its data protection system |
| **Level 2 Governance, Roles & Responsibilities** | The Company pursues the objectives defined on the Strategy level, implementing a data protection governance model consistent with its core business and emphasising the importance given within the data protection organisation to the roles and responsibilities of key players such as the Data Protection Officer. |
| **Level 3 Processing inventory, data management & transfers** | The Company identifies all data processing activities carried out internally, as well as data transfers between companies of the same group and third parties and prepares the Record of Data Processing.<br>The Company monitors and identifies the means used for processing and any transfers of data to non-EU countries. |
| **Level 4 Policies & procedures** | The Company ensures the protection, control and management of personal data processing through the adoption of a set of policies and procedures designed to bring about the proper development of these processes, in line with GDPR requirements (e.g.: Data breach management procedure). |
| **Level 5 Risk management, DPIA, Privacy By design, Audit & Certifications** | In accordance with the GDPR, the Company applies a risk-oriented approach when determining its planning processes and its methodologies. This involves risk analysis or impact assessments (privacy screening and DPIA) when it conceives a new product/service or amends an existing one.<br>Moreover, compliance with the GDPR is guaranteed by regular audits of the DP system and may be confirmed by audit reports/certifications. |
| **Level 6 Training & Awareness** | The Company draws up a data protection training plan and creates a high level of awareness across the business thus enabling its employees to understand and apply the rules established in relation to data protection. Training & Awareness plans are also defined at corporate level. |

# 7 THE DATA MANAGEMENT MODEL

Personal data protection regulations involve many different requirements. These include measures to safeguard Data Subjects (information notice, consent, management of rights), organisational requirements (impact assessment, "privacy by design & by default" approach, the register of processing activities, data breach management procedures) and security requirements. Moreover, certain types of processing are subject to compliance with the specific requirements of the local Supervisory Authorities which Group companies must monitor constantly in order to adapt their data management model to meet local regulatory requirements.
This section sets out the guidelines for compliance with the requirements of the General Data Protection Regulation.

## 7.1 INFORMATION REQUIREMENTS

In order to guarantee correct and transparent processing of personal data, the Controller is required to provide the Data Subject in advance with a series of information, specifically mentioned in the Regulation (in terms of Art. 13 of the GDPR):

- the identity and the contact details of the Controller;
- the contact details of the Data Protection Officer (DPO);
- the purposes of the processing;
- the legal basis for the processing with specific reference, if applicable, to any "legitimate interests" pursued;
- the recipients and categories of recipients of the Personal Data (within the doValue Group or third parties);
- where applicable, the fact that the Controller intends to transfer personal data to a third country;
- the period for which the personal data will be stored, or the criteria used to determine that period;
- the rights granted to the Data Subject and how to exercise them;
- where the processing is based on consent, the existence of the right to withdraw consent at any time (without affecting the lawfulness of processing based on consent before its withdrawal) and how it is possible to withdraw consent;
- the right to lodge a complaint with the supervisory authority;
- whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, and the possible consequences of failure to provide such data
- the existence of automated decision-making, including profiling, the logic involved and the consequences for the Data Subject.

Pursuant to Article 14 of the GDPR, where the data have not been obtained directly from the data subject, the information shall also specify the categories of personal data processed and source of the data.

The information shall be provided to the Data Subject at the time of collection of the personal data or, at the latest, within a month of obtaining the data where they were not obtained directly from the Data Subject.

Each Group Company shall determine the information to be given to the data subjects, for all processing in respect of which that company acts as Controller, while continuously monitoring whether any changes to the means of processing result in the need to update the information.

## 7.2 LAWFULNESS OF PROCESSING AND CONSENT

Any processing of data must have an appropriate legal basis (the lawfulness of processing in terms of Art. 6 of the GDPR).

One condition for the lawfulness of processing is that it has been authorised by the Data Subject, by giving **consent to processing**.

Consent must be obtained in the form and using the methods provided for by the GDPR and it must be demonstrable i.e. the Controller must be able to demonstrate that the Data Subject has given its consent.

Pursuant to Article 7 of the GDPR, consent is considered valid when the following requirements are met:

- Free: the Data Subject shall always be in a position to be able to refuse to grant its consent to performance of certain processing activities; in particular, the execution of a contract or the performance of a service may not be conditional upon the granting of consent to the processing of data not necessary for execution of the contract;
- Specific: each processing operation which, in the absence of another basis for the lawfulness of processing, requires the consent of the data subjects shall be subject to specific consent;
- Informed: the consent shall be preceded by the provision of information on the data processing and the purposes of the consent given and, in any case, by the data subject's review thereof; the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language;
- Clear: the data subject's intention to consent to the processing of personal data relating to him or her shall be expressed by means of an affirmative statement or act;
- Explicit: consent to the processing of certain sensitive shall be given explicitly.

The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing until that time; it shall be possible for consent to be withdrawn easily and promptly.

The types of processing that require consent include, for example, the use of data for commercial purposes or marketing of company or third party products and services, as requested through completion of forms on company web sites or via printed forms, the transmission of personal data to doValue Group companies in case of processing not performed for accounting and administrative purposes (as defined in whereas 48 of the GDPR), the transmission to credit information systems of positive data regarding the regularity of payments of clients with financing relationships.

There are other situations of lawful processing where personal data may be processed even **without consent.** For example, these include where the Processing:

- is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
- is necessary for compliance with a legal obligation to which the Controller is subject;
- is necessary for the purposes of the legitimate interests pursued by the Controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data.

In all cases where the data are processed in order to satisfy a request by the Data Subject e.g. a request for contact or information, performance of a service or fulfilment of contractual obligations, the response to a complaint, or where the data are processed to comply with other laws or regulations applicable to the company (e.g.: customer due diligence for anti-money laundering purposes, registration in lists required under regulations on market abuse, compliance with checks and corporate communications for members of governance bodies and checks required by law in relation to related parties), it is not necessary to request and obtain the consent of the data subject.

If the personal data are processed by a Group company in the capacity of Controller, the transfer of the data to another Group company acting as Processor based on an intercompany service agreement is permitted without requesting the consent of the data subjects.

Finally, in all cases where the data are processed by the Group companies in the capacity of (Third Party) Processors e.g. credit management and recovery on behalf of Principals or servicers for SPVs, it is not necessary to request the consent of the data subject to the data processing performed in the capacity of Processor on the assumption that, where necessary, consent has already been requested and validly obtained by the Controller.

## 7.3 MANAGEMENT OF RIGHTS OF DATA SUBJECTS

In compliance with the GDPR, the doValue Group guarantees recognition of the following rights of data subjects (as defined by Articles 15-21 of the GDPR):

- ✓ *Right of access*: the data subject has the right to obtain confirmation as to whether or not personal data concerning him or her are being processed, and where that is the case, to access the personal data;
- ✓ *Right to rectification*: the data subject has the right to obtain the rectification of inaccurate personal data concerning him or her or to have incomplete personal data completed, taking account of the purposes of processing;
- ✓ *Right to erasure*: the data subject has the right to obtain the erasure of personal data concerning him or her. Note that data whose retention is justified or necessary for legal purposes cannot be erased (e.g. where a customer requests erasure but there is an ongoing legal dispute between it and the Company, the Company may legitimately retain the customer's data, notwithstanding the request);
- ✓ *Right to restriction of processing*: the data subject has the right to obtain the restriction of processing where the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data; or where the data subject has objected to processing, pending the verification whether the legitimate grounds of the controller override those of the Data Subject;

- ✓ *Right to data portability*: the data subject has the right to receive the personal data concerning him or her in a structured, commonly used, and machine-readable format and the right to transmit those data to another controller without hindrance;
- ✓ *Right to object*: the Data Subject has the right to object at any time to processing of personal data concerning him or her for any or all of the purposes for which they were collected. In particular, the data subject has the right to amend his or her consent and, subsequently, to stop any operation or set of operations which is performed, whether or not by automated means, such as collection, recording, organisation, storage, consultation, adaptation or alteration, selection, retrieval, comparison, use, restriction, communication, dissemination, erasure, or destruction, even if not recorded in a database;
- ✓ *Right not to be subjected to an automated decision-making process*: the data subject has the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

For each of the above rights, the doValue Group companies, as Controllers, shall adopt appropriate internal procedures and tools in order to:

- provide a response to the data subject without undue delay in respect of requests received, while justifying to the data subject any delays or failures in providing a response
- manage requests from data subjects within the company while performing appropriate retrieval, amendment, or erasure of the personal data;
- inform any third-party controllers to which the data have been communicated of the requests of the data subject.

Group companies are required to provide a response to the exercise of rights by data subjects whose data are processed by them as Controllers or as Processors where this is specifically requested by the Controller in the Data Protection Agreement (DPA).

It is understood that any requests to exercise rights made by data subjects may not regard personal data referring to third parties, except in particular circumstances (for example, through a legal representative or a lawyer).

In compliance with the GDPR, the LOCAL DPO acts as contact for data subjects exercising their rights and the response to be provided to the data subjects shall be agreed in advance with the LOCAL DPO.

In cases where doValue Group companies operate as third-party Processors (e.g. in relation to credit recovery activities), they must be able to provide the Controller with support in managing requests from data subjects on the basis of the duties set out in the relevant service agreements and in any associated operating instructions. The methods for use in dealing with requests by data subjects are determined on a local level in specific internal rules and regulations.

## 7.4 MANAGEMENT OF DATA RETENTION

In accordance with the aforementioned principle of the restriction of processing, the data shall be stored for the minimum period necessary for the purposes of their processing (Data Retention). In order to ensure that the personal data are not stored for longer than is necessary, the Controller shall establish a deadline for their erasure – this deadline may vary depending on the type of data and the purposes of processing – and implement

appropriate technical and organisational measures to guarantee compliance with the maximum retention period established.

The following shall be taken into account when determining the retention period:

- retention requirements established by law (e.g. privacy, obligation to retain tax records, retention period for accounting records, correspondence, contracts);
- purposes of collection and processing in relation to business and operating requirements;
- instructions given by the Controller (e.g. Principals/SPVs) for data processed in the capacity of Processors (e.g. debtors' data).

Where a Group company intends to stop carrying out one or more processing activities performed as an autonomous Controller, the Personal Data previously used in the context of such operations shall be destroyed or anonymised (where applicable), except for compliance with legal obligations or for defence purposes.

Where the doValue Group companies operate as Processors, the requirements contained in the Data Processing Agreement (DPA) for erasure of the data provided by the Controller are respected.

The specific internal regulations set out Data Retention requirements for the various types of Data / Processing.

## 7.5 DATA PROTECTION BY DESIGN AND BY DEFAULT - DATA PROTECTION IMPACT ASSESSMENT (DPIA)

In order to safeguard the rights and freedoms of natural persons in relation to the processing of their personal data, the GDPR requires the controller to adopt internal policies and implement measures that satisfy the principles of data protection by design and data protection by default.

In particular, the "**Data Protection by design**" principle provides that, taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing, as well as risks of varying likelihood and, both at the time of the determination of the means for processing and at the time of the processing itself, the Controller shall implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this GDPR and protect the rights of data subjects.

The "**Data Protection by default**" principle involves implementing appropriate technical and organisational measures to ensure that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility.

The principles of Data Protection by Design and by Default must be integrated into the entire Group organisation. Therefore, all of the companies shall pay attention so that the development of new products and services and the use of support tools undergo a preliminary check to assess whether any planned data processing takes place in compliance with general and local regulatory requirements: this requires great awareness of the fact that each corporate structure will have to make its contribution to the correct and prompt application of the principles described above.

In more detail, from the planning phase of a new product/service, of the implementation of new stools or of significant changes to means of Data Processing, insofar as possible, while taking into account the state of the art, implementation costs and risks relating to the specific processing, it is necessary:

- to ensure that, under the default set-up of processes/systems, only those Personal Data necessary for each specific purpose of processing are processed;
- to ensure that, under the default set-up of processes/systems, the Personal Data processed are made accessible only to those parties who have to process them in relation to the purposes for which they were collected;
- to consider the entire lifecycle of the Personal Data during which they are processed, from collection until erasure, also taking due account of their transfer, storage, adaptation or alteration, consultation, and communication.

In order to guarantee application of the principles of Privacy by design and Privacy by default within each Group company, it is necessary for each company to adopt its own methodology for determining which processing activities involve a high risk for the data subjects and assessing the impact thereon (Data Protection Impact Assessment). Based on the results of this analysis, each company shall identify appropriate technical and organisational security measures which, once applied, shall mitigate the possible impact on the data subject caused by a loss of confidentiality, integrity, and availability of personal data.
If the company is acting as a Processor, it shall help make all data of interest available to the controller so that it can perform the impact assessment.

## 7.6 REGISTER OF PROCESSING ACTIVITIES

A complete list of Data Processing activities carried out by the Group Companies whether as Controllers or Third-Party Processors and the related purposes is contained in the Register of Processing Activities.

The Register contains at least the following information:

*with regard to Processing carried out as Controller*

- the name and contact details of the controller and, where applicable, the joint controller, the controller's representative, and the data protection officer;
- the purposes of the processing;
- a description of the categories of Data Subjects and of the categories of personal data;
- the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;
- where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and the documentation of appropriate safeguards;
- where possible, the envisaged time limits for erasure of the different categories of data;
- where possible, a general description of the technical and organisational security measures.

*with regarding to Processing carried out as Processor*

- the name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and, where applicable, of the controller's or the processor's representative, and the data protection officer;
- the categories of processing carried out on behalf of each controller;
- where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and the documentation of appropriate safeguards;
- where possible, a general description of the technical and organisational security measures.

The LOCAL DPO is responsible for updating and storing in electronic form the official version of the Register of Processing Activities, also so that it can be made available to the Authority in case of an inspection.

## 7.7 DATA BREACH MANAGEMENT

A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned. Therefore, as soon as the controller becomes aware that a personal data breach has occurred, the controller should notify the personal data breach to the supervisory authority without undue delay and, where feasible, not later than 72 hours after having become aware of it (unless the controller is able to demonstrate, in accordance with the accountability principle, that the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons). Where such notification cannot be achieved within 72 hours, the reasons for the delay should accompany the notification. The notification should at least contain:

- a description of the nature of the personal data breach including, where possible, the categories and approximate number of data subjects concerned, and the categories and approximate number of personal data records concerned;
- communication of the name and contact details of the Local DPO or other contact point where more information can be obtained;
- a description of the likely consequences of the personal data breach;
- a description of the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where the doValue Group companies operate as Processors, they shall promptly inform the Controller of any data breaches within the time period provided for in the Data Protection Agreement (DPA). They shall also provide the Controller with all such information about the breach necessary to notify the event to the Supervisory Authority.

For example, possible Personal Data breaches may regard:

- destruction of electronic data or printed documents (intended as irreversible loss of data with their restoration confirmed as impossible), resulting from logical erasure (e.g. wrongful deletion of data during a manual or automated intervention) or physical damage (e.g. breakage of electronic memory devices, fire/flooding at premises where contracts and other customer documents are stored);
- loss of data as a result of the loss/theft of IT support devices (e.g. laptop, HD, memory card) or of contractual documentation or other printed documents (originals or copies);

- unauthorised access or intrusion to information systems (e.g. contact management systems managed by call centres) by exploiting vulnerabilities in internal systems and communications networks or by compromising or improperly obtaining authentication credentials (e.g. user id and password) to access systems;
- unauthorised amendment of data, resulting, for example, from improper interventions on information systems or human intervention;
- disclosure of data and documents to unauthorised third parties, possibly unidentified. This may result, for example, from providing information – possibly oral information – to persons other than the legitimate party (without the written authorisation of that party), from sending invoices or other contractual or executive documents to parties other than the intended recipient, or from the improper management of IT support devices.

If the internal assessment or audit identifies a high risk for the rights and freedoms of the data subject, exposing it to particular risks in light of the data involved in the data breach, the data subject shall be informed directly without undue delay. The communication to the data subject shall describe in clear and plain language the nature of the personal data breach and contain at least the name and contact details of the DPO, the likely consequences of the breach and the measures taken or proposed to be taken to address the personal data breach.

Communication to the data subject is not required if any of the following conditions are met:

- the controller has implemented appropriate technical and organisational protection measures and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;
- the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of Data Subjects is no longer likely to materialise;
- it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

The Supervisory Authority may still ask that the communication to the data subjects be made.

Each doValue Group company shall adopt internal procedures and tools to detect, combat and manage any security incidences that involve a data breach. Moreover, such internal procedures shall specific the methodology to be followed in assessing the data breach, the means of escalation to corporate governance bodies and the means of notification of the event to the local supervisory Authority and, possibly, to the data subjects, as well as the means of notification to the Controller if the company is acting as Processor.

## 7.8 SECURITY MEASURES

In the course of the Processing activities carried out, the Controller and the Third-Party Processor shall, pursuant to Article 32 of the GDPR, adopt all measures necessary to protect the Personal Data. They shall guarantee:

- the implementation of measures to protect the networks, the systems, and the software with which the Personal Data are processed. For example:

  - user profiling and segregation and access protection solutions such as to ensure that Personal Data can be accessed and processed only by parties that need to process them
  - data pseudonymisation, obfuscation and encryption;
  - service continuity solutions capable of guaranteeing the availability and integrity of data (backup, Disaster Recovery, etc.);
- Testing and periodical assessment of the effectiveness of the procedures and measures implemented;
- Implementation of solutions capable of detecting unauthorised attempts to access Personal Data in order to guarantee compliance with the GDPR requirements on Data Breaches;
- Adoption of solutions for the tracking of activities on Personal Data that are consistent with the applicable legal requirements.

## 7.9 TRANSFERS OF DATA OUTSIDE THE EU

When the GDPR came into force, it introduced a uniform level of Personal Data protection across the European Union and permitted the free circulation of data within EU countries.

However, when Personal Data are transferred from the European Union to Controllers and Processors or to other recipients in countries outside the European Union, the Regulator requires the same level of protection of natural persons as that guaranteed in the European Union.

Therefore, the Personal Data of the Data Subject may be transferred to non-EU countries in the following circumstances, for example:

- transfers to countries which, according to the European Commission, guarantee an appropriate level of Personal Data protection;
- transfers between companies belonging to the same corporate group in the presence of *Binding Corporate Rules (BCR)*, where applicable, or between companies that have signed the "standard clauses" for the protection of Personal Data approved by the Commission;
- transfers necessary for the execution of a contract concluded between the data subject and the controller or for the performance of pre-contractual measures adopted at the request of the Data Subject;
- transfers necessary for the conclusion or execution of a contract signed between the controller and another natural or legal person in favour of the data subject;
- transfers necessary to assert, exercise or defend a right in legal proceedings.

If none of the specific cases above applies, the Data transfer must be explicitly approved by the Data Subject.

Therefore, during the initial phase of a Processing activity or during said activity, it is particularly important for the Group companies to check where the Data Processing takes place, especially where it involves third parties that will have to communicate in which country, they are performing the processing.

## 7.10 SPECIFIC PROCESSING

Each Group Company shall continuously monitor whether the local data protection Authorities issue data protection laws and regulations that are more restrictive than the European Regulation. In such cases, the Controller, with support from the LOCAL DPO, shall assess whether the data processing methods adopted are compliant with the new local regulations and, if they are not, it shall take appropriate action to achieve compliance.

# 8 CONTROL FRAMEWORK

To ensure that organisations have a clear structure that separates the functions that define guidelines from those responsible for their execution, regulators are increasingly calling for a 'three lines of defence' governance model that ensures strong and effective internal control and to guarantee multiple levels of protection.

The figure below represents the Group's data protection control framework:

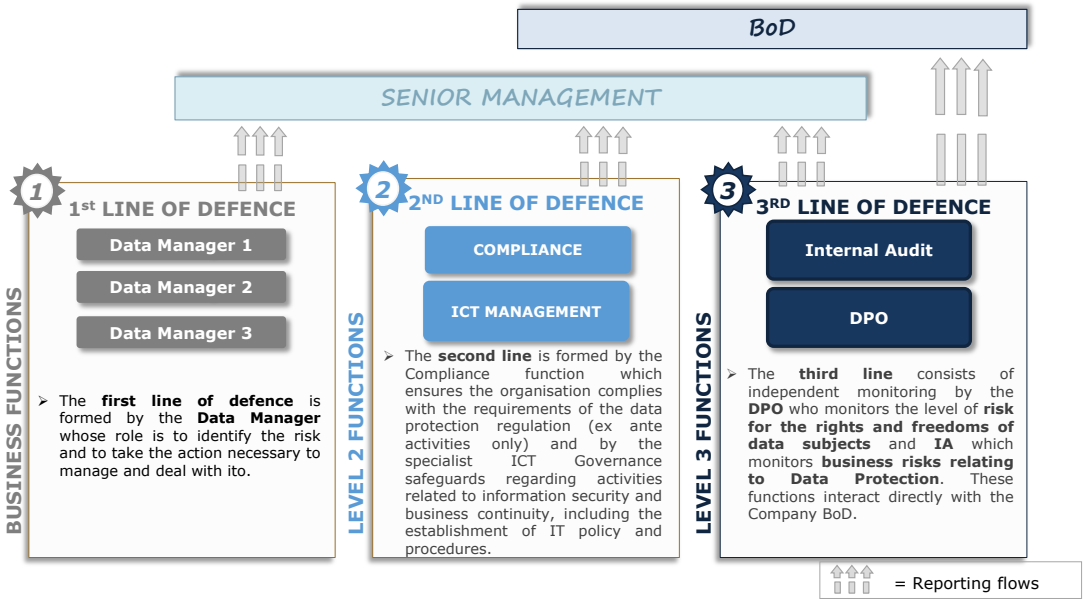



*Fig.10: Data Protection Control Framework*

The Global DPO establishes and maintains a third-level common control framework for all of the Group Companies at the service of the Global DPO and the Local DPO that use it as part of their oversight activities. The oversight activities carried out by the Global DPO and Local DPOs are aimed at determining the risk level in relation to the rights and freedoms of Data Subjects.
The control framework includes specific control activities that shall be tested by the Local DPO.
The control activities defined in the framework are divided into the following categories:

1. GDPR Strategy and Responsibility;
2. Register of processing activities;

3. Determination of legal basis for processing;
4. Consent, propriety, and transparency;
5. Rights of data subjects;
6. Delimitation of data retention;
7. Training and awareness;
8. Data breaches and incident management;
9. Privacy by Design & Privacy by Default;
10. Data Protection Impact Assessment (DPIA);
11. Management of third parties;
12. Security measures;
13. Transfer of personal data.

The Local DPO shall adapt the Framework controls at a local level, on the basis of the specific characteristics of the organisation. Specific control activities shall be added, as necessary, in order to test the compliance of the company Data Protection system with any applicable regulations issued by the Local Authority.
The verifications can be planned on all personal data processing carried out by the company over several years, ensuring however that each year the following are included in the scope of the audit

- processing operations presenting a high (inherent) risk for the rights and freedoms of Data Subjects.
- a subset of processing operations presenting an (inherent) risk for the rights and freedoms of Data Subjects Not high.

Upon completion of these activities, the Local DPO shall produce a report addressed to the local Board of Directors and shall inform the Global DPO of the results of the monitoring activities and of any specific, significant events that occurred during the period in question.

# 9 PENALTIES

Infringement of the General Data Protection Regulation exposes the Controller and/or the Processor open to various types of liabilities and resulting penalties (administrative and/or criminal), depending on the rules that have been breached. Occasionally Data Subjects compensation may be required in case they suffered material or immaterial damages caused by an infringement of the regulation and risk suffering reputational harm.
The GDPR has significantly increased the amount of the administrative penalties, raising them to a maximum of the higher of Euro 20 million or 4% of total worldwide revenue in the previous year. In each case, the Supervisory Authority may decide whether to apply the administrative fines in addition to other non-financial penalties, or in place of such penalties. In any case, pursuant to Art. 83 del GDPR, the administrative fines shall be effective, proportionate, and deterring. Therefore, when determining the amount of the fine, the Authority takes account of a series of factors including the nature, gravity and duration of the infringement, the intentional or negligent character of the infringement, any relevant previous infringements, any action taken by the controller or processor to mitigate the damage suffered by data subjects, the degree of cooperation with the supervisory authority in order to remedy the infringement and mitigate its possible adverse effects, the categories

of personal data affected by the infringement; the manner in which the infringement became known to the supervisory authority, any other aggravating or mitigating factor applicable to the circumstances of the case e.g. financial benefits gained or losses avoided, directly or indirectly, from the infringement.