Procedure for the processing of personal data

Applicable as of 26 April 2021

Summary

1. Introduction 2

1.1 Purpose of the document 2
1.2 Purpose of the process 3
1.3 Subjects and roles 3

2. Processes 5

2.1 Risk analysis 5
2.2 Data Privacy Impact Assessment (DPIA) 5
2.3 Register of processing activities 6
2.4.1 Appointment of the DPO 7
2.4.2 Appointment of the 1st level Authorized Person 7
2.4.3 Appointment of the Manager 7
2.4.4 Appointment of the 2nd level Authorized Persons 7
2.4.7 Management of the appointment deed 8
2.5 Information management and consent collection 9
2.8 Management of the rights of the interested party 12
2.9.1 Nofitication in case of data breach 13
2.9.2 Preventive consultation in case of high residual risk downstream of the DPIA 15
2.10 Periodic checks 15
2.11 Inspections and checks by the Authority 16

References

[01] ANIMA - Functional Chart
[02] ANIMA - Privacy Policy - GDPR
[03] ANIMA - IT security and corporate data protection

Definitions

Client Back Office *- external party taking care, in outsourcing, of the administrative activities of clients for the UCITS set up by Anima Sgr and for the "Arti & Mestieri" Pension Fund.*

Authority - *Independent administrative authority that supervises the correct processing of personal data. To this end, it prescribes necessary or appropriate changes to make the treatments adapt to the current regulations, signals to Parliament and the Government the opportunity of regulatory interventions to protect the interested parties, examines complaints, reports and appeals, carries out checks also at the request of the citizen performs inspections and checks.*

"Privacy by design" and "privacy by default" - *data protection by design and by default (Article 25 GDPR).*

1. Introduction

1.1 Purpose of the document

This document governs the processing of personal data in accordance with the "ANIMA - Privacy - GDPR" policy (hereinafter "Policy") and the regulations in force on the subject, in accordance with the reference regulatory framework on personal data protection (EU) no. 2016/679 of the European Parliament and of the Council of 27 April 2016 (hereinafter, "GDPR") relating to the protection of individuals with regard to

the processing of personal data as well as the free circulation of such data and repealing Directive 95/46 / CE, as implemented in Italy by Legislative Decree 101/2018.

1.2 Purpose of the process

The processes are designed to ensure compliance with the principles of the GDPR, with the commitment to implement the best practice standards in terms of personal data protection.

The operating rules contained in this document apply to any form of data processing and are binding for all employees involved in the processing of the same in the management of products (including also the "Arti e mestieri" Pension Fund), and in rendering services and are binding for all employees and all third parties involved in the data treatment.

In carrying out their activities, all company functions are required to abide by the rules of ordinary diligence and to implement operating behaviors that comply with current legislation.

1.3 Subjects and roles

The organizational model adopted by Anima SGR (the "Company") provides for the following roles, illustrated in detail in the Policy to which reference should be made:

- **Data Controller**: the Company in the figure of the General Manager
- **Joint Data Controllers**: two or more Data Controllers who jointly determine the purposes and means of data processing by defining their respective responsibilities in a written document.
- **Data Processor**: appointed third party suppliers
- **Data Protection Officer (DPO)** - external consultant
- **Level I Authorized Persons**: Head of the Legal and Corporate Affairs Service and the Head of the Information Technology Division
- **Level II Authorized Subjects**: employees, temporary workers and interns;
- **Special Level II Authorized Subjects**: Level II Authorized Subjects employed in one of the following divisions / services:
  - Legal and Corporate Affairs
  - Human Resources (function carried out by Anima Holding)
  - Personal Administration (function carried out by Anima Holding)
  - Management secretariat (function carried out by Anima Holding)
  - Internal Audit
  - Compliance
  - Anti-money laundering
  - Customer Support and Services
  - Support and Services for the Business
  - Financial Investigations and Successions
  - GP Back Office
  - UCITs, Mandates and Pension Fund Back Office
  - Controls NAV calculation and operating controls
  - Marketing
  - Communication & Marketing.
- **System Administrator**: specifically appointed personnel belonging to the Information Technology & Facility Management Division.

The functions indicated in the table below participate in the process. Coordination and supervision is entrusted to the "process owner".

The management of relations with the Authority for the protection of personal data is the responsibility of the DPO, with the support of the Legal and Corporate Affairs Service.

PRIVACY - GDPR		
PROCESSES	**PROCESS OWNER**	**OTHER SUBJECTS**
RISKS ANALYSIS	INFORMATION TECHNOLOGY	DPO AND THE INVOLVED FUNCTION ON A CASE BY CASE
IMPACT EVALUATION (DPIA)	LEGAL & CORPORATE AFFAIRS AND DPO	INVOLVED FUNCTION ON A CASE BY CASE
REGISTER OF THE PROCESSING ACTIVITIES	DPO	LEGAL & CORPORATE AFFAIRS
APPOINTMENTS	LEGAL & CORPORATE AFFAIRS	HR MANAGEMENT SYSTEM ADMINISTRATORS
INFORMATION MANAGEMENT AND CONSENT COLLECTION	LEGAL & CORPORATE AFFAIRS	CHART § 2.5
SUPPLIERS' EVALUATION	PURCHASE	LEGAL & CORPORATE AFFAIRS DPO AND INTERNAL AUDIT
CORPORATE CULTURE AND TRAINING PROGRAMS	HUMAN RESOURCES	-
MANAGEMENT OF THE RIGHTS OF THE INTERESTED PARTY	LEGAL & CORPORATE AFFAIRS	DPO INFORMATION TECHNOLOGY
NOTIFICATIONS TO THE AUTHORITY FOR THE PROTECTION OF PERSONAL DATA	LEGAL & CORPORATE AFFAIRS INFORMATION TECHNOLOGY	DPO
PERIODIC CHECKS	DPO	LEVEL I AUTHORIZED PERSONS

2. Processes

In accordance with the provisions of the General Regulations for the Protection of Personal Data (hereinafter "**GDPR**"), the Company has implemented the following compliance processes:

1. Risk analysis
2. Impact assessment (Data Privacy Impact Assessment, DPIA)
3. Register of processing activities
4. Appointments management
5. Information management and consent collection
6. Evaluation of suppliers appointed as external managers
7. Corporate culture and training programs
8. Rights management of the interested party
9. Notifications to the Authority for the protection of personal data
10. Periodic checks

2.1 Risk analysis

Pursuant to art. 32 of the GDPR, the Data Controller must have adequate technical and organizational measures to ensure a level of security appropriate to the risk. These measures must be implemented taking into account the state of the art and the costs of implementation, the nature, object, context and purpose of the processing, as well as the probable risk to the rights and freedoms of individuals.

Therefore, in its Privacy management system, the Company periodically checks the implementation of the minimum security measures in accordance with the GDPR and with the principle of proportionality recalled by the Authority, carrying out an analysis on the potential risks in relation to the processing of data. personal (so-called risk analysis). If necessary, the Company adopts the security measure that guarantees the best protection of the rights and freedoms of the individuals concerned.

The risk analysis is carried out according to the following phases:

- identification of company assets;
- assessment of threats and vulnerabilities and related impacts on the confidentiality, integrity and availability of personal data;
- identification of risk exposure;
- identification of security measures to mitigate risks.

The risk analysis is prepared by the Information Technology Division on an annual basis or whenever it is possible to identify new threats or vulnerabilities following periodic checks on internal systems.
The risk analyzes and the results of the security checks are suitably filed by the Head of the Information Technology Division in a specific network folder.

For details on the security measures adopted by the Company, consult the ANIMA organizational procedure - IT security and company data protection - tools and rules of conduct.

2.2 Data Privacy Impact Assessment (DPIA)

Pursuant to art. 35 of the GDPR, the Data Controller carries out an impact assessment or Data Privacy Impact Assessment ("DPIA") when a type of processing presents a high risk for the rights and freedoms of individuals, when it involves the use of new technologies taking into account the nature, object, context and purpose of the processing.

The assessment activities include a preliminary mapping of the personal data processing carried out within the Company. For each processing, the data retention period is identified based on the purposes of the processing itself, a degree of risk is established on the basis of internally agreed estimates and in accordance with the provisions of art. 32 of the GDPR.

The processing of personal data for which the degree of risk associated with them is high are subject to impact assessment.

If the risks associated with the processing subject to the impact assessment are mitigated by the technical-organizational measures put in place by the Data Controller to comply with the provisions of the GDPR, thus mitigating or avoiding the risks to the rights and freedoms of the data subjects, it is not necessary to proceed with the prior consultation with the Authority pursuant to art. 36 of the GDPR (see paragraph 2.9.2 "Prior consultation in case of high residual risk downstream of the DPIA"). Conversely, if downstream of the impact assessment, the risk associated with the processing remains high even in the presence of technical and organizational measures, it is necessary to proceed with sending the prior consultation.

The responsibility for the evaluation process lies with the Data Controller.

The SGR is supported by the DPO regarding the need to proceed or not with an impact assessment of the processing of personal data and in the possible drafting of the associated documentation, having heard the opinion of the internal structures involved in the processing of personal data subject to rating.

With each new processing of personal data, the company function that carries out the new processing activity (not previously recorded in the Register of processing activities - see paragraph 2.3) promptly informs the Legal and Corporate Affairs Service about the existence of the new processing in company.

The Legal and Corporate Affairs Service, in turn, promptly informs the DPO for an opinion on the need or not to proceed with a DPIA pursuant to art. 35 of the GDPR and in order to update the treatment register.

The impact assessments and related documentation are appropriately filed by the Legal and Corporate Affairs Service in a specific network folder.

2.3 Register of processing activities

The processing of personal data identified by the Data Controller is contained in the so-called Register of processing activities (Article 30 of the GDPR).

The Register provides an updated picture of the processing of personal data in place within the Company (including any activities carried out on behalf of another Data Controller as Data Processor) and is essential for any risk assessment and analysis.

It also constitutes a fundamental tool for the application of the new accountability and privacy by default principle provided for by the GDPR (see Policy), becoming an integral part of the Company's personal data management system and acts as a guarantee of compliance with the GDPR in towards the competent authorities.

The Register is kept by the Data Controller and updated quarterly by the DPO, who keeps a copy.

2.4 Appointments

2.4.1 Appointment of the DPO

The Company has a Data Protection Officer (DPO) appointed by the Data Controller of the Parent Company Anima Holding following the board resolution, pursuant to art. 37, 2nd paragraph of the GDPR. The designated person is a professional external to the ANIMA group.

2.4.2 Appointment of the 1st level Authorized Person

The decision whether to designate one or more Level I Authorized Subjects is the responsibility of the Data Controller, who identifies among the Company's staff who, due to experience, ability and reliability, provides a suitable guarantee of full compliance with the law on the matter.

2.4.3 Appointment of the Manager

The appointment of the Data Processor (as an alternative to the assumption by the third party of the privacy role of independent data controller in addition to the Company already Data Controller) is defined in the contracting with the third party supplier of the activities and / or services which involve the processing of data. The appointment follows the verification indicated in paragraph 2.6 regarding the guarantees of the Data Processor required by art. 28 of the GDPR. Verification is handled by the Purchasing and Supplies Service.

2.4.4 Appointment of the 2nd level Authorized Persons

The appointment as Level II Authorized Person is required by company policy at the time of starting work at the Company for all employees, temporary workers and interns (see Policy).

2.4.5 Appointment of the particular 2nd level Authorized Subject

The appointment as a particular Level II Authorized Person is envisaged by company policy at the time of starting work at the Company for all employees, temporary workers and interns who work in one of the following divisions / services:

- Legal and Corporate Affairs
- Human Resources (function carried out by Anima Holding)
- Personal Administration (function carried out by Anima Holding)
- Management secretariat (function carried out by Anima Holding)
- Internal Audit
- Compliance
- Anti-money laundering
- Customer Support and Services
- Support and Services for the Business
- Financial Investigations and Successions
- GP Back Office
- UCITs, Mandates and Pension Fund Back Office
- Controls NAV calculation and operating controls
- Marketing
- Communication & Marketing..

2.4.6 Appointment of the System Administrator

The appointment as **System Administrator** is assessed by the Head of the Information Technology Division on the basis of the subjects who, due to experience, ability and reliability, are considered suitable for exclusive and privileged access to the resources of the company information system.

2.4.7 Management of the appointment deed

The drafting of the so-called "Deed of designation" (in the case of the appointment of the 1st level Authorized Subject) or of the so-called "Deed of appointment" (in other cases), as well as its modification or the drafting of the revocation deed, is handled by the Legal and Corporate Affairs Service. The deed contains the tasks and operating instructions that the designated / appointed person must comply with.

Each deed is signed by the Data Controller.
Each deed is drawn up and delivered to the interested party by:

- **Personnel Administration** for the appointment of:
  - Data Controller for the designation of Level I Authorized Entities;
  - 2nd level Authorized Person and a 2nd level Special Authorized Person.
- **Legal and Corporate Affairs** to the Data Controller for the appointment of the DPO (Data Protection Officer)
- **Head of the Information Technology & Facility Management Division** for the appointment as System Administrator;
- Company function that holds the relationship with the third party, for the appointment as Data Processor;

The same subjects listed above coordinate the acquisition of the countersigned deed for receipt and acceptance by the appointed person.

The deeds are kept by the Legal and Corporate Affairs Service, with the exception of:

- the deed of appointment of the 2nd Level Authorized Person and of the particular 2nd Level Authorized Person, whose conservation is handled by the Personnel Administration Service.
- The deed of appointment of the System Administrator, whose conservation is handled by the Information Technology and Facility Management Division.

The list of appointees - in compliance with the minimization principle enunciated by the GDPR - is updated at least annually by the Personnel Administration Service in order to:

- identify the treatment allowed to the person in charge,
- manage the user profile and authorize access to network folders and company applications.

Each job rotation and new hiring is promptly communicated by the Personnel Administration Service to the System Administrator for the creation of utilities with related accesses, authorized by the Head of the reference office on the basis of what foreseen in the procedure “ANIMA – Cybersecurity and company data protection – Instruments and rules of conduct”.
The permissions to the fileserver folders, once authorized, can only be changed by sending a written request to the helpdeskl or by the manager of the folder or by making the manager himself aware.

System administrators reconcile permissions annually by sending an e-mail to the folder manager who can confirm or ask to change the permissions assigned.

The list of Data Processors, independent data controllers and joint data controllers, is periodically updated and kept by the Legal and Corporate Affairs Service. The list is available in response to requests from the interested parties.

The list of system administrators is kept by the Head of the Information Technology Division and reported in a specific document that can be consulted in the company intranet area in the "Privacy" section. It is made available to the Authority in case of investigations.

2.5 Information management and consent collection

As required by current legislation, and in particular by art. 5 GDPR, the personal data subject to collection are:

1. processed in a lawful, correct and transparent manner towards the interested party ("lawfulness, correctness and transparency ");
2. collected for specific, explicit and legitimate purposes, and subsequently processed in a way that is compatible with these purposes; further processing of personal data for the purposes of archiving in the public interest, for scientific or historical research or for statistical purposes is not considered incompatible with the initial purposes ("purpose limitation"), in accordance in Article 89, paragraph 1 of the GDPR;
3. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ("data collection minimization");
4. accurate and, if necessary, updated; all reasonable steps must be taken to promptly delete or rectify inaccurate data with respect to the purposes for which they are treated ("accuracy");
5. kept in a form that allows the identification of data subjects for a period of time not higher than the achievement of the purposes for which they are processed; personal data can be kept for longer periods provided they are processed solely for the purpose of archiving in the public interest, for scientific or historical research or for statistical purposes, in accordance with art. 89, paragraph 1 of the GDPR, without prejudice to the implementation of technical measures and adequate organizational requirements to protect the rights and freedoms of the data subject ("limited conservation ");
6. processed in such a way as to ensure adequate security of personal data, including the protection, through adequate technical and organizational measures, from unauthorized or unlawful processing from accidental loss, destruction or damage ("integrity and confidentiality").

In order for a treatment to be considered lawful, at least one of the following must be verified conditions:

- the interested party has given consent for one or more specific purposes;
- it is necessary for the execution of a contract with the interested party;
- it is necessary to fulfill a legal obligation incumbent on the owner;
- it is necessary for the protection of the vital interests of the data subject or of another natural person;
- it is necessary for the performance of a task of public interest;
- it is necessary for the pursuit of a legitimate interest of the owner.

To this end, it is sufficient to provide the interested party with appropriate information regarding the processing of personal data, in accordance with the provisions of the GDPR (see articles 12 - 14).

The consent from the interested party is however always necessary in the following cases:

- the data is processed for purposes other than those necessary for the execution of the contract with the interested party and to comply with legal obligations (for example, the communication of data to third parties)
- the object of the processing is personal data so-called details (Article 9 GDPR)

The Company has provided various types of information and forms for consent to the processing of personal data, diversified according to the purpose of the processing, set out in the following table:

INFORMATION AND CONSENT FORM	RESPONSIBLE COMPANY FUNCTION
General privacy disclaimer (published on the company's website)	• Communication & Marketing
Disclaimer and consent for the registration to the reserved area of the website	• Communication & Marketing
Disclaimer and consent for the registration to the newsletter (reserved area of the website)	• Communication & Marketing
Disclaimer and consent form for subscribers	• Operating development and support • Institutional and Wholesale Division
Disclaimer and consent form for company representatives	• Legal and Corporate affairs
Disclaimer and consent form for job posting applicants	• HR (Selection, Training and Development)
Disclaimer and consent form for company advisors	• Function where the advisor works
Disclaimer and consent form for employees, stagiaires and term contractors	• HR Management
Disclaimer and consent form for other collaborators	• HR Management
Disclaimer and consent form for suppliers	• Purchase department • Outsourcers Monitoring (with reference to the outsourcing agreements)

The process is divided into the following phases:
- Drafting
- Information delivery
- Consent collection
- Archiving

The Legal and Corporate Affairs Service must prepare and keep updated the information for adressees and the consent forms, after sharing the contents with the competent corporate function, based on the different operational area.
The information is signed by the Data Controller.

The delivery of the information to the interested party and, where applicable, the consent form to the processing, is carried out by the company structure responsible for the relationship with the third party, in relation to the different operating environment (see table above).

The collection of the consent of the interested party is handled by the company service that holds the relationship with the recipient of the information.
Upon receipt of the information form, it is necessary to verify that it has been signed and is complete with the expression of consent to the processing of data. A copy of the consent / information form is kept by the company service that took care of the consent collection.

2.6 Evaluation of the suppliers appointed as Data Processors

In compliance with the principle set out in art. 28 of the GDPR, the Data Processors are appropriately assessed by the Purchasing and Supply Service - on the basis of an adequacy assessment questionnaire - after signing the contract, in the case of a new supplier, or annually, in the case of an existing supplier. .

Adherence to a code of conduct approved pursuant to art. 40 of the GDPR or an approved certification mechanism referred to in art. 42 of the GDPR can be used as a sufficient element of guarantee for the external manager.

The Data Processors are appointed by contract, pursuant to art. 28 GDPR, prepared by the Legal and Corporate Affairs Service.

Annually the Company shall select at least 2 suppliers in order to verify the requirements set out in art. 28, in particular, the Company verifies that the Data Processor:

• commits to respect the entire content of this procedure
processes personal data in accordance with the documented instructions of the Data Controller
• guarantees that the persons authorized to process personal data are committed to confidentiality or have an adequate legal obligation of confidentiality;
• adopts all the measures required pursuant to article 32;
• comply with the conditions set out in the appointment to have recourse to another Data Processor;
• takes into account the nature of the processing, assisting the Data Controller with appropriate technical and organizational measures, in order to satisfy the Data Controller's obligation to follow up on requests for the exercise of the data subject's rights;
• assists the Data Controller in ensuring compliance with the obligations referred to in articles 32 to 36, taking into account the nature of the processing and the information available to the controller;

This verification will take place through the sending of a questionnaire by the Purchasing and Supplies Service. The answers to the questionnaire will be analyzed by the DPO who will express his opinion through a verification report.

The Company reserves the right to have a third party carry out an audit on those Data Processors who deal with particular categories of data or who have not fully answered the questionnaire. This activity will be coordinated by the Internal Audit Service.

The suppliers appointed as Data Processors are indicated in a special list kept by the Legal and Corporate Affairs Service.

2.7 Corporate culture and training programs

In accordance with the provisions of art. 29 of the GDPR, the personnel in charge and the profiles of responsibility in terms of Privacy must be appropriately trained by the Data Controller.
Adequate training of the subjects appointed to process personal data is considered an organizational measure necessary to ensure an adequate level of security in the processing of personal data.

The Company approves an annual training plan aimed at all persons in charge of data processing.
Training on the subject of Privacy is mandatory and is subject to the staff being hired.
In case of need, online update courses are provided.

2.8 Management of the rights of the interested party

The interested party can exercise their rights respecting the conditions and limits of the law.
According to the GDPR, the rights of the data subject are:

- Right to access data
- Right of rectification
- Right to be forgotten
- Right to limit the processing
- Right to data portability
- Right to object

For definitions, refer to the company Privacy Policy.

In addition to the above, art. 22 of the GDPR states that - where not required for other purposes listed in paragraph 2 of the same article - the interested party has the right not to be subjected to a decision based solely on automated processing, including profiling, which produces legal effects concerning him. or which significantly affects his person in a similar way.

Applications for the exercise of these rights can be sent to the dedicated e-mail address dpo@animasgr.it governed by the DPO who will promptly notify the Legal and Corporate Affairs Service, or to the privacy@animasgr.it mailbox managed and monitored by the Business Service Legal and Corporate.

The receipt and management of the response to the interested party is carried out by the Legal and Corporate Affairs Service within the deadlines set by the GDPR.
The Legal and Corporate Affairs Service retrieves all data and information useful to provide feedback to the interested party, availing itself, where necessary, of the collaboration of other corporate functions which must provide the information in their possession in writing and promptly.

In particular, in case of exercising the right of data portability, the Legal and Corporate Affairs Service, following the appropriate internal checks and the opinion of the DPO, will send the customer the data collected directly from the Sgr (if a direct customer, the present in the reserved area and in the due diligence form, if a customer of the network, the data present in the subscription, redemption and switch form).

The reply to the interested party is the responsibility of the Legal and Corporate Affairs Service, which keeps the correspondence with the interested party, together with all the information elements used to provide feedback for a period of ten years.

The reply to the interested party is provided at the latest within one month of receiving the request (therefore the date of receipt must be documented). The deadline can be extended up to a further two months (three months in total), if necessary, taking into account the complexity and number of requests. The owner of the Processing informs the interested party of this extension and of the reasons for the delay, within one month of receipt of the request.

In providing feedback, the following principles must be respected:
a) facilitate the exercise of the rights of the interested parties;
b) provide a prompt response;
c) identify the Data Subjects if the Data Controller has reasonable doubts;
d) payment for the exercise of rights: depending on the request, a copy of the Data subject to processing must be provided, free of charge; in case of further copies requested by the interested party, the Data Controller may charge a reasonable cost-based fee (preferably predetermined and disclosed to the interested party); if requests of the interested party are manifestly unfounded or excessive (as demonstrable by the Data Controller), in particularly due to their repetitive nature, it is possible to: i) charge a reasonable fee taking into account the administrative costs incurred to provide the information or communication to take the required action; ii) refuse to comply with the request.

The requests of the interested party are archived by the Legal and Corporate Affairs Service after having obtained the opinion of the DPO.

2.9 Notifications to the Data Protection Authority

2.9.1 Nofitication in case of data breach

A "data breach" pursuant to the GDPR is a security breach that involves, accidentally or unlawfully, the destruction, loss, modification, unauthorized disclosure or access to personal data transmitted, stored or otherwise processed.

In case of violation (Article 33 GDPR), the Data Controller will have to carry out a series of assessments aimed at understanding whether the "data breach" involves a risk for the rights and freedoms of the natural persons involved and if it involves a high risk for the interested party.

Following these assessments, the Data Controller must:

- if the violation involves a risk for the rights and freedoms of individuals: notify the data breach to the Authority without undue delay and where possible within 72 hours from the moment in which he became aware of the violation;
- if the violation also involves a high risk for the freedom and rights of the data subjects, promptly communicate the event to the latter and in any case without undue delay;
- if there are no risks to the rights and freedoms of individuals, do not notify the data breach to the competent Authority, but keep track of it in a specific register of violations ("Register of Violations"), keeping adequate documentation relating to the event and indicating the reasons why you have chosen not to send the relevant notification.

It is the responsibility of the Legal and Corporate Affairs Service to update the Register of Violations.

The internal company Division / Service that becomes aware of a personal data breach, notifies the Legal and Corporate Affairs Service in advance, which will promptly consult with the DPO.

In addition, IT security violations are monitored by the Information Technology Division through periodic first level automatic and manual checks.

In the event of a violation at the systems of the outsourcer appointed as Data Processor, the violation must be promptly reported by the outsourcer to the Information Technology Division.

The assessment of the need to send the notification to the Authority is conducted according to the following logic and considerations:

- identification of the type of violation (loss, tampering, disclosure of personal data);
- assessment of the nature, sensitivity and volume of the personal data involved;
- assessment of the ease of identification of the natural persons concerned;
- assessment of the severity of the consequences for the individuals concerned;
- considering the characteristics of the natural persons concerned;
- considering the number of natural persons involved;
- considering the characteristics of the data controller and the type of personal data processed

The notification to the Authority is handled by the Data Controller who will use the help of the DPO, in accordance with the requirements of the law.

2.9.2 Preventive consultation in case of high residual risk downstream of the DPIA

According to the GDPR, the Data Controller must necessarily consult the supervisory authority - before proceeding with the processing - if the outcome of the impact assessment on data protection (pursuant to Article 35 of the GDPR and governed by processes in paragraph 2.2 of this procedure) highlights a high residual risk (so-called preventive consultation).

The Data Controller communicates to the Authority:

- where applicable, the responsibilities of the Data Controller, the joint controllers and the Data Processors;
- the purposes and means of the envisaged processing;
- the measures and guarantees envisaged to protect the rights and freedoms of the data subjects;
- the contact details of the data protection owner;
- the data protection impact assessment referred to in Article 35;
- any other information requested by the supervisory authority

The supervisory authority provides, within eight weeks of receiving the request for consultation, a written opinion to the Data Controller and the Data Processor.
The supervisory authority may extend the aforementioned period by six weeks, taking into account the complexity of the envisaged treatment. However, the supervisory authority has the duty to inform the Data Controller and, where applicable, the Data Processor of this extension, together with the reasons for the delay, within one month of receiving the request for consultation.

Until the opinion is obtained from the Supervisory Authority, it is not possible to proceed with the processing of personal data subject to prior consultation.

2.10 Periodic checks

Pursuant to the GDPR, it is the task of the DPO, with the support of the Level I Authorized Subject (for the parts of their respective competence) to carry out a formal and substantial verification of the policies and procedures adopted by the SGR and subsequent periodic checks for internal reporting to the Data Controller.

The checks are conducted annually taking into account the results of previous audits, any complaints received, any data breach notifications to the Authority and the activities implemented in relation to the security of the data processed.

The audit plan is shared annually by the DPO with the Data Controller.

Any recommendations or observations of non-compliance found by the DPO during the verification phase must be managed by the corporate functions involved in the process being assessed, providing subsequent evidence to the DPO of the measures adopted for their resolution.

Furthermore, the first level Authorized Subjects, for the parts of their respective competence, check on a sample basis:

- compliance with the instructions received from the persons in charge of processing e
- compliance with the instructions and compliance with the law by the Data Processors.

The checks are conducted through the use of a questionnaire. The evidence collected in this way is suitably filed by the first level Authorized Subjects, each for the checks pertaining to them.

2.11 Inspections and checks by the Authority

By virtue of the powers of inspection and control the Privacy Authority can:

- request information and documents;
- access databases and archives and carry out inspections and checks in the places where the treatments take place;
- to order the Data Controller and the Data Processor to provide any information necessary for the performance of its duties;
- conducting investigations in the form of data protection audits;
- notify the Data Controller or the Data Processor of the alleged violations of this regulation;
- obtain, from the Data Controller or the Data Processor, access to all personal data and all information necessary for the performance of its duties;
- obtain access to all the premises of the Data Controller and the Data Processor, including all the tools and means of data processing, in compliance with Union law or the procedural law of the Member States.

Furthermore, the Authority has the following corrective powers:

- send warnings to the Data Controller or to the Data Processor on the fact that the envisaged treatments may likely violate the provisions of this regulation
- issue warnings to the Data Controller and Data Processor or to the Data Processor if the processing has violated the provisions of this regulation;
- to order the Data Controller or the Data Processor to satisfy the requests of the interested party to exercise their rights deriving from this regulation;
- to order the Data Controller or the Data Processor to conform the processing to the provisions of this regulation, if necessary, in a certain manner and within a certain period;
- to order the Data Controller to communicate to the interested party a violation of personal data;
- impose a provisional or definitive limitation on processing, including a prohibition on processing;
- order the rectification, deletion of personal data or limitation of processing pursuant to Articles 16, 17 and 18 and the notification of these measures to the recipients to whom the personal data have been disclosed pursuant to Article 17, paragraph 2, and of article 19;
- to impose a pecuniary administrative sanction
- order the suspension of data flows to a recipient in a third country or an international organization.

Activities can originate from:

- reports or complaints received by the Authority from the interested parties;
- needs for further investigation that emerged during the examination of appeals;
- initiative of the Authority;
- random checks, to verify the state of implementation of the law in certain sectors.

The maintenance of relations with the Privacy Authority and the coordination of the activities deriving from any required investigations and checks, is the responsibility of the DPO with the support of the Legal and Corporate Affairs Service, assisted if necessary by other company functions based on the area of competence.