ANIMA Holding S.p.A.

Privacy - GDPR

Applicable from 20/12/2021

Contents

References

[1] AH - Code of Corporate Governance
[2] AH - Privacy Policy - GDPR
[3] AH - Data Security and Corporate Data Protection

Changes to the Document

Versions	Date	Description of Changes
00	24/09/2018	First issue
01	09/05/2019	Adaptation of Organisational Structure, New DPO and Board Approval
02	16/06/2021	Adaptation of Organisational Structure, Regulatory adaptation, Resolution of Compliance issue
03	20/12/2021	Revision to resolve Internal Audit issue

Definitions

- ***Data Protection Authority*** - Independent administrative authority that supervises the correct processing of personal data. To this end, it prescribes changes that are necessary or appropriate to bring processing operations into line with current regulations, notifies Parliament and the Government of the advisability of regulatory interventions to protect the data subjects, examines complaints, reports and appeals, carries out investigations also at the request of members of the public, and performs inspections and audits.

- ***'Privacy by design' and 'privacy by default'*** - data protection by design and by default (Art. 25 GDPR).

1. Introduction and Overview

1.1. Objective of this document

This document governs the processes regarding the processing of personal data in accordance with the "AH - Privacy - GDPR" policy (hereinafter the "Policy") and the applicable regulations in accordance with the data protection framework laid down in Regulation (EU) No. 2016/679 of the European Parliament and of the Council of 27 April 2016 (hereinafter "**GDPR**") on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC, as implemented in Italy by Legislative Decree 101/2018.

1.2. Objective of the process

The objective of the process is to ensure compliance with the principles of the GDPR by aligning the company with the market standards on personal data protection.

The rules contained in this document apply when carrying out any form of data processing, and apply to all employees and third parties involved in the processing operations.

In the performance of their activities, all corporate functions or appointed third parties are required to comply with the rules of ordinary diligence and to conduct their operations in accordance with the regulations in force.

1.3. Actors and roles

The organisational model adopted by Anima Holding S.p.A. (the "Company") provides for the following roles, which are illustrated in detail in the Policy, to which please refer.

- **Data Controller** - the Company, in the person of the Chief Executive Officer.
- **Joint Data Controllers:** two or more Data Controllers who jointly determine the purposes and methods of the data processing, by defining their respective responsibilities in a written document.
- **Data Processor** - the duly appointed third-party providers.
- **Data Protection Officer (DPO)** - external consultant.
- **Level I Authorised Persons** - Head of the Legal and Corporate Affairs Office and Head of the Information Technology Unit.
- **Level II Authorised Persons** - employees, temporary workers and interns.
- **Special Level II Authorised Persons** - the Level II Authorised Persons employed in one of the following functions**:**
  - Legal and Corporate Affairs
  - Recruitment, Training and Development
  - Personnel Administration
  - Executive Administration Office
  - Internal Audit
  - Compliance
  - Institutional Marketing, Communication and Web.

- **System Administrator** - specially-appointed Information Technology personnel

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

The management of relations with the Data Protection Authority is the responsibility of the DPO, with the support of the Legal and Corporate Affairs Office.

PRIVACY - GDPR		
PROCESSES	**PROCESS OWNER**	**OTHER ACTORS**
RISK ASSESSMENT	Information Technology	DPO and the relevant corporate function
IMPACT ASSESSMENT (DPIA)	Legal and Corporate Affairs DPO	Corporate functions concerned
REGISTER OF PROCESSING ACTIVITIES	DPO	Legal and Corporate Affairs
MANAGEMENT OF APPOINTMENTS	Legal and Corporate Affairs	Personnel Administration System administrators
MANAGEMENT OF PRIVACY POLICIES AND CONSENT FORMS	Legal and Corporate Affairs	Table paragraph 2.5
EVALUATION OF SUPPLIERS APPOINTED AS EXTERNAL DATA PROCESSORS	Purchases and Supplies	Legal and Corporate Affairs DPO and Internal Audit

CORPORATE CULTURE AND TRAINING PROGRAMMES	Recruitment, Training and Development Personnel Administration	-
MANAGING DATA SUBJECT RIGHTS	Legal and Corporate Affairs	DPO Information Technology
NOTIFICATIONS TO THE DATA PROTECTION AUTHORITY	Legal and Corporate Affairs Information Technology	DPO
PERIODIC AUDITS	DPO	Level I Authorised Persons

2. Processes

In accordance with the requirements of the General Data Protection Regulation (hereinafter '**GDPR**'), the Company has implemented the following compliance processes:

1. **Risk Analysis**
2. **Data Privacy Impact Assessment (DPIA)**
3. **Record of processing activities**
4. **Management of Appointments**
5. **Management of consent forms and privacy policies**
6. **Evaluation of suppliers appointed as data processors**
7. **Corporate culture and training programmes**
8. **Managing the rights of the data subject**
9. **Notifications to the Data Protection Authority**
10. **Periodic audits**

2.1 Risk assessment

Under Article 32 of the GDPR, the Data Controller is required to take appropriate technical and organisational measures to ensure a level of security appropriate to the risk. These measures must be implemented taking into account the state of the art, the costs of implementation, the nature, object, context and purpose of the processing, and the likely risk to the rights and freedoms of natural persons.

As part of its privacy management system, the Company thus periodically verifies the implementation of minimum security measures, in compliance with the GDPR and with the principle of proportionality indicated by the Data Protection Authority, by conducting a risk assessment in relation to the processing of personal data. Where necessary, the Company adopts the security measures that best protect the rights and freedoms of the natural persons concerned.

The risk assessment involves the following steps:
- the identification of company assets;
- the assessment of threats and vulnerabilities and their impact on the confidentiality, integrity and availability of the personal data;
- the identification of exposure to risk;
- the identification of security measures to mitigate those risks.

The risk analysis is prepared by the Information Technology function, on annual basis or whenever new threats or vulnerabilities are detected after a periodic audit of the internal systems.

The risk assessments and results of the security audits are then archived by the Information Technology Manager in a special network folder.
For details on the security measures adopted by Anima Holding, refer to the organisational procedure *AH - Information Security and Corporate Data Protection - Policies and Rules of Conduct*.

2.2 Data Privacy Impact Assessment (DPIA)

Under Article 35 of the GDPR, the Data Controller is required to carry out an impact assessment or Data Privacy Impact Assessment ('DPIA') whenever a type of processing operation presents a high risk to the rights and freedoms of natural persons, when it involves the use of new technologies taking into account the nature, subject matter, context and purposes of the processing.

The assessment includes a preliminary mapping of the processing of personal data carried out within the Company. For each processing operation, the data retention period is identified on the basis of the purpose of the type of processing. A risk level is then established on the basis of internally agreed criteria and in accordance with Article 32 of the GDPR.

Processing operations with a high risk level are the subject of an impact assessment.

If the risks associated with the processing operation in question are mitigated by the technical-organisational measures put in place by the Data Controller to comply with the GDPR, thereby mitigating or avoiding the risks to the rights and freedoms of the data subjects, no prior notification to the Data Protection Authority is required pursuant to Article 36 of the GDPR (see paragraph 2.9.2 "Prior consultation in case of high residual risk post-DPIA"). Conversely, if after the impact assessment, the risk associated with the processing operation remains high, despite the presence of technical and organisational measures, it is necessary to proceed with the prior consultation.

The responsibility for the risk assessment process lies with the Data Controller.

The Company relies on the advice of the DPO as to whether or not a DPIA is required, and with regard to the drafting of any associated documentation, after consulting the internal departments involved in the data processing operation in question.

The impact assessment and all the associated documentation is drafted and shared with the DPO and the Legal and Corporate Affairs Office. At the end of the impact assessment, the Legal and Corporate Affairs Office submits the documentation for initialling by the corporate function performing the processing operation and for the signature of the Data Controller.

With each new processing of personal data, the corporate function performing the new processing operation (if not previously recorded in the Register of Processing Activities - see Section 2.3) will duly inform the Legal and Corporate Affairs Office of the existence of the new processing operation.

The Legal and Corporate Affairs Office will then inform the DPO, to obtain an opinion as to whether or not a DPIA is necessary pursuant to Article 35 of the GDPR and for the purpose of updating the Register of Processing.

The impact assessments and related documentation are duly filed by the Legal and Corporate Affairs Office in a special network folder.

2.3 Record of processing activities

The personal data processing operations identified by the Data Controller are contained in the Register of Processing Operations (Art. 30 GDPR).

The Register provides an up-to-date picture of the processing of personal data taking place within the Company (including any activities carried out on behalf of another Data Controller, as Data Processor) and is indispensable for any risk assessment or analysis.
It also constitutes a fundamental tool for the application of the new principles of accountability and privacy by default, as envisaged in the GDPR (see Policy); it is an integral part of the Company's personal data management system and is a guarantee towards the competent authorities of the Company's compliance with the GDPR.

The Register is kept by the Data Controller and, if a new processing operation is introduced, the DPO, with the support of the Legal and Corporate Affairs Office, will promptly update it and keep a copy for himself.

2.4 Management of Appointments

2.4.1 Appointment of the DPO

The Company has a Group Data Protection Officer (DPO) who is appointed by the Data Controller following a Board resolution, thus in accordance with Article 37(2) of the GDPR. The designated person is a data protection professional who is external to the Anima Group.

2.4.2 Appointment of Level I Authorised Person

The decision to designate one or more Level I Authorised Persons is the responsibility of the Data Controller, who will identify from among the Company's staff those persons whose experience, capacity and reliability provide an adequate guarantee of full compliance with the relevant law.

2.4.3 Appointment of Data Processor

The appointment of the **Data Processor** (as an alternative to the third party assuming the privacy role of independent data controller in addition to the Company, which is already the Data Controller) is defined at the time of signature of the contract with the third-party provider of the activities and/or services involving the processing of data. The appointment is made subsequent to the checks indicated in paragraph 2.6 concerning the guarantees of the Data Processor as required by Article 28 of the GDPR. The checks are carried out by the Purchasing and Supplies office.

2.4.4 Appointment of Level II Authorised Persons

Appointment as a Level II Authorised Person is required by company policy at the time of commencement of employment with the Company, for all employees, temporary workers and interns (see Policy).

2.4.5 Appointment of Special Level II Authorised Persons

Appointment as a special **Level II Authorised Person** is a requirement of company policy at the time of hiring, for all employees, temporary workers and interns who work in one of the following offices:
- Legal and Corporate Affairs
- Recruitment, Training and Development
- Personnel Administration
- Executive Administration Office
- Internal Audit
- Compliance
- Institutional Marketing, Communication and Web

2.4.6 Appointment of System Administrator

Appointment as **System Administrator** is evaluated by the Head of the Information Technology Unit, for individuals who, by virtue of their experience, skills and reliability, are considered suitable for exclusive and privileged access to the Company's information system resources.

2.4.7 Management of the act of appointment

The drafting of the "act of designation" (in the case of a Level I Authorised Person) or "act of appointment" (in other cases), as well as its amendment or the drafting of the act of revocation, is the responsibility of the Legal and Corporate Affairs Office. The act sets out the tasks and operational instructions to be followed by the designated/appointed person.

Each act is signed by the Data Controller.

Each document is delivered to the person concerned by:
- **Personnel Administration,** for the appointment of:
  - Data Controller for the designation of Level I Authorised Persons;
  - Level II Authorised Person and Level II Special Authorised Person.
- **Legal and Corporate Affairs Office** to the Data Controller for designation as Data Protection Officer (DPO);
- **Head of Information Technology Unit** for appointment as System Administrator;
- **The corporate function that holds the relationship with the third party**, for the appointment as Data Processor.

The persons listed above will coordinate the acquisition of the document, countersigned for receipt and acceptance by the appointed person.

The appointment documents are retained by the **Legal and Corporate Affairs Office**, with the exception of:
- the act of appointment of the Level I and Level II Authorised Person and the Level II Special Authorised Person, which is kept by the Personnel Administration Office;
- the act of appointment as System Administrator, which is kept by the Information Technology Unit.

The list of appointees - in compliance with the principle of minimisation set out in the GDPR - is updated at least once a year by Personnel Administration, in order to:
- identify the processing operations that the person is authorised to carry out,
- manage the user profiles and authorise access to network folders and company software.

Personnel Administration will duly inform the System Administrator of every job rotation and new hire, to allow the creation of new user accounts and accesses, authorised by the Head of the relevant office on the basis of the provisions set out in the procedure "*AH - Information Security and Corporate Data Protection - Tools and Rules of Conduct*", to which please refer for details.
Permissions to access folders on the fileserver, once authorised, can only be changed by written request, to be sent to helpdesk@animasgr.it either by the person responsible for the folder, or by informing the person responsible.
On an annual basis, the system administrators will check the permissions by sending an e-mail to the folder manager, who can confirm or request any changes to the permissions assigned.

The list of Data Processors, Independent Data Controllers and Joint Data Controllers is updated periodically and is kept by the Legal and Corporate Affairs Office. The list will be provided in response to requests from the Data Subjects.

The list of system administrators is kept by the Head of Information Technology and is set out in a special document, which can be consulted on the company Intranet in the 'Privacy' section. It is made available to the Data Protection Authority in the event of an investigation.

2.5 Management of consent forms and privacy policies

As required by current legislation, and in particular by Article 5 GDPR, the personal data collected are:

1. processed in a way that is lawful, fair and transparent towards the data subject ('lawfulness, fairness and transparency');
2. collected for specified, explicit and legitimate purposes, and subsequently processed in a way that is not incompatible with those purposes; any further processing of personal data for archiving in the public interest, scientific or historical research or statistical purposes is, in accordance with Article 89(1) GDPR, not considered incompatible with the original purposes ('purpose limitation');
3. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
4. accurate and, where necessary, kept up to date; every reasonable step must be taken 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');
5. stored in a form which permits the identification of data subjects only for a period of time that does not exceed the purpose for which they are processed; personal data may be stored for longer periods provided that they are processed solely for archiving purposes in the public interest, scientific or historical research or for statistical purposes in accordance with Article 89(1) GDPR, subject to the implementation of appropriate technical and organisational measures required to protect the rights and freedoms of the data subject ("limitation of storage");
6. processed in such a way as to ensure the adequate security of the personal data, including protection, by appropriate technical and organisational measures, against unauthorised or unlawful processing and accidental loss, destruction or damage ('integrity and confidentiality').

At least one of the following conditions must be fulfilled in order for a treatment to be lawful:

- the data subject has given consent for one or more specific purposes;

- the processing is necessary for the performance of a contract with the person concerned;
- the processing is necessary to comply with a legal obligation incumbent on the data controller;
- the processing is necessary to safeguard the vital interests of the data subject or of another natural person;
- the processing is necessary for the performance of a task in the public interest;
- the processing is necessary for the pursuit of a legitimate interest of the data controller.

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

The consent of the data subject is, however, necessary in the following cases:

- the data are processed for purposes other than those necessary for the performance of the contract with the data subject and to fulfil legal obligations (e.g. disclosure of data to third parties)
- the object of the processing is sensitive personal data (Art. 9 GDPR)

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

PRIVACY POLICY AND CONSENT FORM	CORPORATE FUNCTION RESPONSIBLE FOR THE RELATIONSHIP WITH THE DATA SUBJECT
Generic privacy policy (published on the Company's **website)**	• Institutional Marketing, Communication and Web
Privacy policy and consent to registration in the reserved area of the Company's **website**	• Institutional Marketing, Communication and Web
Newsletter and consent policy (reserved area of the Company's **website)**	• Institutional Marketing, Communication and Web
Privacy policy and consent form for officers of the company	• Office of Legal and Corporate Affairs
Privacy policy and consent form for job applicants (first contact after sending CV)	• Human Resources (Recruitment, Training and Development)
Privacy policy and consent form for consultants of the company	• Office of the Company at which the consultant works
Privacy policy and consent form for employees, interns and temporary workers	• Personnel Administration
Privacy policy and consent form for special representatives	• Personnel Administration
Privacy policy and consent form for suppliers of goods or services (if a natural person, sole trader or registered professional)	• Purchases and Supplies

The process consists of the following steps:

- Editing and publication
- Transmission of the policy
- Obtaining of consent
- Archiving

Legal and Corporate Affairs is responsible for preparing and updating the privacy policies and consent forms for the data subjects, after sharing the contents with the relevant corporate function, depending on the operational scope.

The policies are signed by the Data Controller.

The delivery of the privacy policy to the data subject and, where applicable, the consent form for processing, is carried out by the corporate department responsible for the relationship with the third party, depending on the operational scope (see table above).
The obtaining of the data subject's consent is taken care of by the department that has the relationship with the data subject.
Upon receipt of the privacy policy, it is necessary to check that it has been signed and is accompanied by the declaration of consent to the data processing.

A copy of the consent/information form is retained by the company department that obtained the consent.

2.6 Evaluation of suppliers appointed as Data Processors

The appointment as Data Processors pursuant to Article 28 GDPR is made by the Legal and Corporate Affairs Office, which formally obtains it as part of the supply contract.

In compliance with this law, the role of Data Processor is assessed when the contract is signed and, subsequently, their compliance with the requirements of Article 28 will be verified, as set out below.

Where the supplier states that it adheres to an approved code of conduct or approved certification mechanism pursuant to Article 42 of the GDPR, this may, if stated in the contractual documentation, constitute an adequate guarantee for the external data processor. In this case, verification is not necessary.

Procedures for verifying the requirements of the Data Processor

The aim is to verify that the Data Processor meets the requirements of Article 28 of the GDPR and, consequently:

- is committed to complying with the provisions of the GDPR;
- processes personal data in accordance with the documented instructions of the Data Controller;
- can guarantee that the persons authorised to process the personal data are bound by a non-disclosure obligation or have an adequate legal obligation of confidentiality;
- takes all the measures required pursuant to Article 32;
- meets the conditions set out in the appointment to use another Data Processor;
- takes into account the nature of the data processing, by assisting the Data Controller with the appropriate technical and organisational measures, in order to fulfil the Data Controller's obligation to comply with requests to exercise the rights of the data subject;
- assists the Data Controller in ensuring compliance with the obligations set out in Articles 32-36, taking into account the nature of the processing and the information available to the Data Controller;

Annually, the Legal and Corporate Affairs Office, in cooperation with Purchasing and Supplies, will select at least two suppliers to be audited.

This verification takes the form of a questionnaire sent by Purchasing and Supplies, who must check that the questionnaire is completed and will then send it to the DPO. The answers to the questionnaire will be analysed by the DPO, who will express his opinion in a formal report to be shared with Legal and Corporate Affairs.

If the replies to the questionnaire are incomplete, Legal and Corporate Affairs will ask Internal Audit to intervene with the supplier in order to resolve any issues, in cooperation with the DPO. After this, Internal Audit will prepare a report to be forwarded to Legal and Corporate Affairs, which is responsible for keeping the audit documentation in accordance with Article 28 of the GDPR.

The suppliers appointed as Data Processors are named in a list kept by Legal and Corporate Affairs.

In order to monitor the list of suppliers appointed as Data Processors, every three months Legal and Corporate Affairs will request a list of active contracts, which is updated by Purchasing and Supplies whenever the Company signs a contract with a new supplier.

2.7 Corporate culture and training programmes

In accordance with Article 29 of the GDPR, the authorised persons and Privacy roles must be appropriately trained by the Data Controller.
Adequate training of anyone in charge of processing personal data is considered a necessary organisational measure, to ensure an adequate level of security in the processing of personal data.

The Company will approve an annual training plan for all the authorised data processors.
Privacy training is compulsory and provided to staff at the time of hiring.
Online refresher courses will be provided if necessary.

2.8 Managing data subject rights

The data subject can exercise their rights within the conditions and limits laid down by law.

According to the GDPR, the rights of the data subject are:

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

Please refer to the company's Privacy Policy for the definitions.

In addition, Article 22 of the GDPR states that - unless required for other purposes listed in paragraph 2 of the same Article - the data subject has the right not to be subjected to a decision based solely on automated processing, including profiling, which produces legal effects concerning them or significantly affects them in a similar way.
Requests for the exercise of these rights can be forwarded to the dedicated mailbox: dpo@animasgr.it which is controlled by the DPO, who will promptly notify Legal and Corporate Affairs, or to the mailbox privacy@animasgr.it, which is managed and monitored by Legal and Corporate Affairs.

The receipt and handling of the response to the data subject is carried out by Legal and Corporate Affairs within the deadlines set in the GDPR.

Legal and Corporate Affairs will retrieve all the data and information useful for providing a response to the Data Subject, availing itself, where necessary, of the cooperation of other corporate functions, which must promptly provide the information in their possession in writing.

Giving feedback to the data subject is the responsibility of the Legal and Corporate Affairs Office, which will store the correspondence with the data subject, together with all the feedback documents, for a period of ten years.

The reply to the data subject must be provided within one month of receipt of the request (therefore the date of receipt must be documented). This deadline may be extended by up to a further two months (three months in total) if necessary, taking into account the complexity and number of requests. The Data Controller will inform the Data Subject of this extension and of the reasons for the delay within one month of receipt of the request.

The following principles must be observed when providing feedback:
a) the exercise of the data subjects' rights must be facilitated
b) the response must be timely
c) the Data Subjects must be identified, if the Data Controller has reasonable doubts
d) payment for the exercise of rights: depending on the request, a copy of the processed Personal Data must be provided, free of charge; if the Data Subject requests additional copies, the Data Controller may charge a reasonable contribution to the administration costs (preferably pre-determined and made known to the Data Subject); if the Data Subject's requests are manifestly unfounded or excessive (as demonstrable by the Data Controller), or in particular are repetitive, the Data Controller may: (i) charge a reasonable fee taking into account the administrative costs incurred in providing the information or communication or taking the requested action; (ii) refuse to comply with the request.

The requests from the data subject will be filed by Legal and Corporate Affairs, after obtaining the opinion of the DPO.

2.9 Notifications to the Data Protection Authority

2.9.1 Notification in the event of a data breach

A 'data breach' within the meaning of the GDPR is any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data transmitted, stored or otherwise processed.

In the event of a breach (Art. 33 GDPR), the Data Controller is required to carry out a series of assessments in order to determine whether the data breach poses a risk to the rights and freedoms of the individuals involved and whether it poses a high risk to the data subject.
Following these assessments, the Data Controller will:

- if the data breach poses a risk to the rights and freedoms of the individuals: advise the Data Protection Authority without undue delay and where possible within 72 hours of becoming aware of the breach;
- if the breach also entails a high risk to the freedom and rights of the persons concerned, notify the data subjects of the event without undue delay;
- if there is no risk to the rights and freedoms of the individuals, the competent authority will not be notified but a record of the data breach will be kept on the ('Data Breach Register'), with adequate supporting documentation and an indication of why no notification was given.

It is the responsibility of Legal and Corporate Affairs to update the Data Breach Register.
The corporate function that becomes aware of a personal data breach will report it in advance to Legal and Corporate Affairs, who will promptly consult with the DPO.

IT security breaches are monitored by the Information Technology Unit, through periodic automated and manual Level I checks.
In the event of a data breach on the systems of an outsourcer appointed as a Data Processor, the outsourcer must immediately report the incident to the Information Technology Unit.

The assessment as to whether or not the Data Protection Authority needs to be notified will be conducted according to the following logic and considerations:

- identification of the type of breach (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 individuals concerned;
- assessment of the seriousness of the consequences for the individuals concerned;
- the characteristics of the individuals concerned;
- the number of people involved;
- the characteristics of the data controller and the type of personal data processed.

The report to the Data Protection Authority will be handled by the Data Controller, who will be assisted by the DPO as required by law.

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

According to the GDPR, the Data Controller must compulsorily consult the supervisory authority - before proceeding with the data processing - if the outcome of the data protection impact assessment (pursuant to Article 35 of the GDPR and governed by the processes in Section 2.2 of this procedure) shows a high residual risk (this is called 'prior consultation').

The Data Controller will inform the Data Protection Authority:
- where applicable, of the responsibilities of the Data Controller, the joint controllers and the Data Processors;
- the purposes and means of the intended processing;
- the measures and safeguards in place to protect the rights and freedoms of the data subjects;
- the contact details of the data controller;
- the data protection impact assessment provided for in Article 35; and
- any other information requested by the supervisory authority.

The supervisory authority, within a period of eight weeks after receiving the request for consultation, will provide a written opinion to the Data Controller and the Data Processor.
The supervisory authority may extend this period by six weeks, taking into account the complexity of the intended processing operation. However, the supervisory authority has a duty to inform the Data Controller and, where applicable, the Processor of such an extension, together with the reasons for the delay, within one month of receipt of the request for consultation.

Until the opinion of the Supervisory Authority has been obtained, the personal data subject to prior consultation cannot be processed.

2.10 Periodic audits

Under the GDPR, it is the responsibility of the DPO, with the support of the Level I Authorised Officers (for the parts falling within their respective spheres of competence) to carry out audits, within the framework of an annual plan shared with the Data Controller [1], in order to identify any shortcomings

[1] These audits must include a report, to be issued during the same year to the Authorised Level I Persons and copied to Internal Audit.

in compliance with company policies and practices, ensuring the successful outcome of the corrective actions taken by the internal functions involved in each case.

2.11 Investigations and controls by the Data Protection Authority

By virtue of its powers of investigation and control, the Data Protection Authority can:

- request information and documents;
- obtain access to databases and archives and carry out inspections and audits in the places where processing takes place;
- order the Data Controller and the Data Processor to provide any information it needs to perform its tasks;
- to carry out investigations in the form of data protection audits;
- notify the Data Controller or the Processor of any alleged violations of this Regulation;
- obtain, from the Data Controller or the Data Processor, access to all the personal data and information necessary for the performance of its tasks;
- obtain access to all the premises of the Data Controller and the Data Processor, including all the instruments and means of data processing, in accordance with EU law or the procedural law of the Member States.

In addition, the Data Protection Authority has the following corrective powers:

- it may send warnings to the Data Controller or the Data Processor if the intended processing operations are likely to breach the provisions of this Regulation;
- it may address warnings to the Controller and Processor or Processor where processing operations have breached the provisions of this Regulation;
- it may require the Data Controller or the Data Processor to comply with the data subject's requests to exercise their rights under this Regulation;
- it may order the Data Controller or the Data Processor to comply with the provisions of this Regulation, where applicable, in a certain manner and within a certain period of time;
- order the Data Controller to notify the data subject of a personal data breach;
- impose a temporary or definitive limitation, including a ban on processing;
- order the rectification or erasure of personal data or restriction of processing pursuant to Articles 16, 17 and 18 and the notification of such actions to the recipients to whom the personal data have been disclosed pursuant to Article 17(2) and Article 19;
- impose a fine;
- order the suspension of data flows to a recipient in a third country or to an international organisation.

These activities may originate from:

- reports or complaints received by the Data Protection Authority from the data subjects;
- the need for further investigation arising from the examination of appeals;
- the initiative of the Authority;
- spot checks, to verify the state of implementation of the law in certain areas.

The maintenance of relations with the Privacy Guarantor and the coordination of activities resulting from any inspections and checks required, is the responsibility of the DPO with the support of Legal and Corporate Affairs, assisted if necessary by other corporate functions according to their area of competence.