Group Privacy Policy

This Policy ensures rules and guidelines for the management of the processing of personal data, in accordance with the provisions of the European Regulation (EU) No. 2016/679 (GDPR) and local regulations governing the matter, by the DIAGRAM Group Companies subject to the application of the GDPR.

Identification:

Type	Group Policy (Class 2)		
Visibility	☐ Confidential	☐ Internal	☑ Public
Status	☐ In process	☐ Draft	þPublished

Approvals:

Activities	Name	Date
Approved by	Francesca Gusti	26/11/2025
Published by	Gloria Ghilardi	26/11/2025

Summary

1 SCOPE AND PURPOSE 4
2 RESPONSIBILITIES 4
3 PRIVACY PRINCIPLES 4
4 GLOSSARY 7
5 GENERAL PRINCIPLES 10
5.1 Definition of personal data 11
6 PRIVACY ORGANISATIONAL MODEL (M.O.P.) 12
6.1 Foreword 12
6.2 Roles within the DIAGRAM Group 12
6.3 Data Controller 13
6.4 Data Processor (Group Companies and Third Parties) 13
6.5 Group Companies 13
6.6 Third Parties 13
6.7 Data Protection Officer 14
6.8 Privacy Focal Points of the DIAGRAM Group Companies 14
6.9 Authorised Processors 15
7 REGISTER OF PROCESSING ACTIVITIES 15
8 MANAGEMENT MODEL 16
8.1 Collection 16
8.1.1 Purposes 16
8.1.2 Legal basis 16
8.1.3 Consent 16
8.1.4 Execution of a contract 17
8.1.5 Fulfilment of a legal obligation 18
8.1.6 The privacy policy 18
8.2 Processing - General principles 19
8.2.1 Processing by Third Parties 19
8.2.2 Transfers outside the EU 19
8.2.3 Cookies and similar technologies 20
8.2.4 Security 20
8.2.5 Specific processing - Termination of Processing - Deletion and Destruction 21
9 Rights of the data subject and feedback 22
9.1 Right of access 22
9.2 Right of rectification 22
9.3 Right to erasure 22
9.4 Right to restriction of processing 22
9.5 Right to data portability 23
9.6 Right to object 23

9.7 Reply to the applicant and time limits 23
10 Operating Instructions 24
11 Privacy by design & by default 24
12 Data Protection Impact Assessment (DPIA) 25
13 Data Transfer Impact Assessment (TIA) 25
14 Data Breach Notification 25
15 Inspections by the Supervisory Authority 26
16 Rules of conduct in case of inspection activities 26
17 Training 27
18 Audit 27
19 Sanctions 27

1 SCOPE AND PURPOSE

This Policy applies to Diagram S.p.A. (also "Parent Company") and/or its Italian and foreign Subsidiaries (hereinafter referred to individually as the "Company" or "Subsidiary" and collectively as the "DIAGRAM Group"), subject to the application of the GDPR, in activities involving the processing of personal data in the course of performing business activities.

This Policy also applies to subsidiaries based in the United Kingdom, as the relevant law, the UK GDPR, has been deemed 'adequate' until 27 December 2031 by the European Commission, with a level of protection considered 'essentially equivalent'. The articles cited in the EU GDPR also apply to the UK GDPR. Any specific details will be specified on a case-by-case basis.

It is expressly stated that, due to the specific nature of the activities carried out by Agriconsulting S.p.A. and its subsidiaries and the particular subjective and objective context in which they operate, the aforementioned companies will not adopt this Policy.

The purpose of the document is to regulate personal data processing activities within the DIAGRAM Group, in order to ensure full compliance with the provisions dictated by European Regulation No. 2016/679 (GDPR)

2 RESPONSIBILITIES

Group management is responsible for ensuring compliance with this Policy. In particular, all persons involved in the processing of personal data must contribute to the protection of personal data by applying this Policy and the "*Privacy Principles*" indicated below.

This Policy may be implemented and supplemented, where necessary, following indications by the Legal & Compliance Function of DIAGRAM S.p.A., the Focal Point, and by the DPO where present for the Head of the Group and the Subsidiaries, with reference to what is stated in Chapter 6 of the Privacy Organisational Model (MOP) .

3 PRIVACY PRINCIPLES

Processing and purposes	The DIAGRAM Group processes personal data in a lawful, correct and transparent manner, for the achievement of business purposes that are determined, explicit and legitimate, and takes reasonable measures to ensure that personal data are accurate and, if necessary, updated.
Third Parties	Third parties (suppliers, business partners, consultants) that enter in any capacity into a business relationship with the companies of the DIAGRAM Group and, by virtue thereof, carry out operations of processing personal data on their behalf, are designated as **Data Processors** and are contractually bound to comply with measures for the security and confidentiality of the data, and to refrain from any use or disclosure that is not authorised by the DIAGRAM Group. The DIAGRAM Group attaches particular importance to the protection of the **confidentiality** of personal data, soliciting the contribution of all collaborators, internal and external, in the achievement of this objective.

Communication of personal data

The personal data conferred may be **communicated** to third parties in order to comply with legal obligations, in execution of orders from public authorities or in order to assert or defend a right in court, as well as within the companies that are part of the DIAGRAM Group for business needs and for internal administrative purposes, including the processing of personal data of customers and employees.
Personal data may be communicated to third parties, in their capacity as autonomous Data Controllers or Data Processors, with **the consent of** the Interested Parties, if required by law, and in any case subject to adequate information specifying the purposes of the processing. Personal data shall not be **disseminated**.

Storage

Personal data are retained only for the time necessary to achieve the purposes for which they were collected or in accordance with the terms required by law or necessary to enforce a legal claim. Personal data are retained in accordance with the Group Retention Policy, made available to employees in the Team, in the Company Regulations section, unless there are different different storage equirements dictated by local regulations.

Labour relations employment

With reference to the data that the Companies process in the performance of **labour relations**

the DIAGRA Group uses personal data only for the achievement of related purposes (such as, for example, execution of the labour relationship, benefits, tax, welfare and social security fulfilments, hygiene and safety at work; training and career development activities, performance evaluation; use of personal data, including photographic and video images, for institutional purposes).

Commercial and marketing activities

In compliance with the principles of **lawfulness, correctness and transparency,** and with the prior **consent** of the Data Subject if required by law, the DIAGRAM Group may process personal data for the achievement of commercial and marketing purposes (such as, for example, sending advertising material and other promotional and marketing initiatives; direct sales activities; statistical processing).

Security

The DIAGRAM Group adopts **secure technologies and reasonable precautions to protect personal data** against undue disclosure, alteration or improper use. The protections activated are aimed, in particular, at minimising the risks of destruction and loss, even accidental, of data, unauthorised access or processing that is not permitted or does not comply with the purposes of collection.

Periodic **risk analysis** activities are carried out within the Group to check adherence to the defined security standards and, if necessary, to adopt new security measures following organisational changes and technological innovations or changes in the type of data collected. Security measures are **constantly monitored** and **periodically checked**.

Self - Assessment

The DIAGRAM Group carries out a **periodical self-assessment** in order to verify that this Policy is applied throughout the Group and that all persons within the Group comply with these *Principles*.

Compliance

In defining *the Privacy Principles*, the DIAGRAM Group complies with European Regulation no. 679/2016 and, in general, with the applicable laws and regulations that protect the confidentiality of personal data in the jurisdictions in which DIAGRAM S.p.A. or its Subsidiaries operate. Specific jurisdictions may require the DIAGRAM Group to supplement this Policy to comply with local laws.

Contact

For any questions and/or concerns regarding the application of this Policy, please contact the DIAGRAM Group DPO (dpo@diagramgroup.it) or the Focal Point Diagram (privacy@diagramgroup.it).

4 GLOSSARY

In order to facilitate understanding of this document, the following is a list of some keywords and their definitions:

System Administrator	Natural person entrusted with the management and/or maintenance of a computer and data processing system or its hardware and software components, as defined by the General Provision of the Italian Privacy Guarantor of 27 November 2008 and subsequent amendments and additions;
Control Authority (or Authority)	The Authority referred to in Article 51 of the European Data Protection Regulation, i.e. one or more independent public Authorities appointed by a Member State to monitor the application of the Regulation in order to protect the fundamental rights and freedoms of natural persons with regard to the processing of personal data. In Italy, the independent supervisory authority is the Garante per la protezione dei dati personali (the "Garante Privacy");
Authorised processor	Natural person authorised to materially carry out processing operations on personal data on behalf of the Controller. All employees who, by virtue of their duties, are authorised to process personal data.
Standard Contractual Clauses	Guarantee instrument prepared by the European Commission in order to regulate and legitimise the transfer of personal data outside the European Economic Area.
Communication	The giving of knowledge of personal data to one or more persons other than the data subject, the representative of the Controller or the Controller not established in the territory of the European Union, the persons authorised to process personal data under the direct authority of the Controller or the Controller or expressly designated, in any form whatsoever, including by making them available, consulting them or by interconnection;
Subsidiary	all Companies directly or indirectly controlled by DIAGRAM S.p.A. At the time of writing of this document, the "affiliates" to which this document is applied are: Abaco Spa, Abaco UK, Abaco Malta (Bizfront srl), Agronica Srl and Netsens Srl.
Data Processing Agreement ("DPA")	An agreement for the processing of personal data signed between a Data Controller and a Data Processor and aimed at regulating the data, purposes and methods of processing as well as the obligations and responsibilities of the parties;
Data Protection Impact Assessment ('DPIA')	Assessment of the risks associated with the processing of personal data and of the impact that the occurrence of the identified risks may have on the rights and freedoms of those affected by the processing;
Data Protection Officer or 'DPO' ***(or 'DPO')***	entity designated by the data controller or processor to perform support and control, advisory, training and information functions in relation to the application of the Regulation. Co-operates with the Authority and is the point of contact, also in relation to data subjects, for matters related to the processing of personal data
Identifying data	Identification data are data by means of which it is possible to obtain the direct identification of the data subject. By way of example, both codes derived from personal data (e.g. tax code) and the unique codes assigned to a person on the basis of predefined criteria (e.g. customer codes) are identification data;

Personal data	Any information relating to an identified or identifiable natural person ("data subject"), even indirectly, by reference to any other information, including a name, an identification number, location data, an online identifier or to one or more factors specific to his physical, physiological, genetic, mental, economic, cultural or social identity
Sensitive/particular data	Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, as well as processing of genetic data, biometric data intended to uniquely identify a natural person, data concerning a person's health or sexual life or sexual orientation
Disclosure	The disclosure of personal data to unspecified persons in any form, including by making them available or consulting them
General Data Protection Regulation ("GDPR")	The "General Data Protection Regulation", i.e. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, which establishes the European regulatory framework in the field of personal data protection;
DIAGRAM Spa Group	Diagram Spa and all its subsidiaries
Headquarters ("HQ")	Registered office of DIAGRAM S.p.A.
Data subject	The natural person who is identified or identifiable, directly or indirectly, by personal data and to whom the processed data refers;
Legitimate Interest Assesment ("LIA")	Balancing the interests of the data controller who processes personal data on the basis of its legitimate interest against the rights and freedoms of the data subjects to whom the processed personal data relate;
Privacy Organisational Model ('P.O.M.')	Means a set of rules, procedures organisational and technical measures adopted to ensure compliance with data protection and privacy regulations
Crisis Committee	Coordination group in the event of incidents relating to: the application of privacy regulations, the Group's cyber security, safety at work, composed of representatives of the relevant corporate functions (CEO, RSPP, HR, Legal&Compliance, CTO/CISO, DPO)
Privacy Focal Point ("FPP")	A natural person, designated at Diagram Group level and valid for all the Subsidiaries, appointed as a point of contact between the Company itself and the DPO of each Subsidiary, where present, in order to facilitate the management of all issues and local specificities concerning the processing of personal data
Data Processor	The subject (natural or legal person) who is appointed as Data Processor in relation to the processing of Personal Data carried out on behalf of the Data Controller, as a result of a formal act of appointment that defines the scope of responsibilities assigned
Sub-processor	The subject (natural or legal person) who carries out the processing activities entrusted to him/her by the Data Processor
Data Controller	The natural or legal person who determines the purposes and means of the processing of personal data. The controller is also responsible for ensuring the implementation of technical and organisational measures to guarantee a level of security appropriate to the risk
Transfer Impact Assessment ('TIA')	Impact Assessment on the transfer of personal data outside the EU and EEA and for which the adequate safeguards for the transfer set out in Chapter V° of the GDPR are not in place.
Transfers of personal	Any transfer of personal data processed or intended to be processed after transfer

data	to a third country outside the EU/EEA for which an adequacy decision has not been issued, including onward transfers of personal data from one third country to another third country
Processing	Any operation or set of operations, carried out without the help of electronic means, concerning the collection, recording, organisation, storage, consultation, processing, alteration, selection, retrieval, comparison, use, interconnection, blocking, communication, dissemination, erasure and destruction of data, whether or not recorded on a database;
Data Protection Impact Assessment (DPIA)	Data Protection Impact Assessment (DPIA) is a process required by the GDPR to assess the risks of a processing of personal data that is likely to present a high risk to the rights and freedoms of individuals. The DPIA includes a description of the processing, an assessment of necessity and proportionality, a risk analysis and the security measures to be taken to mitigate those risks. It is mandatory before starting high-risk processing operations, such as those using new technologies or large-scale monitoring systems.
Data Breach	A breach of security leading accidentally or unlawfully to the destruction, loss, modification, unauthorised disclosure of or access to personal data transmitted, stored or otherwise processed.

5 GENERAL PRINCIPLES

European Regulation No. 2016/679[1] , better known by the acronym GDPR ('General Data Protection Regulation'), is a European Union regulation on the protection of natural persons with regard to the processing of personal data, aimed at uniformly regulating the privacy rights of European citizens.

These rules are designed to strengthen the confidence of data subjects, making them more aware of how personal information about them is used and free to make an informed decision on whether or not to consent to its use[2]

This has a significant impact on the data that are normally collected and managed by the company as part of its normal commercial, marketing, operational and general business activities, as a result of the increased level of protection of personal data - relating to customers and consumers, as well as to employees and collaborators - brought about by the Regulation.

As part of the performance of its business activity, the DIAGRAM Group collects a significant amount of data and confidential information, which it undertakes to process in compliance with all privacy and confidentiality laws in force in the jurisdictions in which it operates.

In particular, the principles expressed in the **DIAGRAM Group's Code of Ethics** state the following: "*We are committed to protecting any sensitive, confidential and proprietary information concerning the Group. Confidentiality is essential to guarantee trust and authenticity, both within the Group and in relations with partners and consumers'*.

The same commitment to confidentiality in the use, processing and safekeeping of data must be assumed and guaranteed by all employees and non-employees who, in the performance of their activities, process personal data on behalf of the DIAGRAM Group.

Employees and collaborators of the DIAGRAM Group, at all levels, are therefore required to recognise whether they are collecting, using, processing, storing or sharing personal data that are subject to protection. They must therefore be aware of the **cardinal principles that govern the processing of personal data**, i.e. that the data

- must be processed lawfully, fairly and transparently vis-à-vis the data subject, in accordance with the specific purposes clearly and comprehensibly described in the privacy statement and on the basis of the lawfulness requirements justifying the processing (including explicit consent to processing, where necessary)
- must be collected for specified, explicit and legitimate purposes and subsequently processed in a way that is not incompatible with those purposes ('purpose limitation principle')
- must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('Principle of minimisation')
- they must be accurate and, where necessary, kept up to date
- must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which they are processed ('Principle of limited storage');
- must be processed in such a way as to ensure adequate security of personal data, including protection - by means of appropriate technical and organisational measures - against unauthorised or unlawful processing and against loss, destruction, alteration, unauthorised disclosure or access that could cause damage.

Compliance with these principles is the responsibility of the **Data Controller**, supported by the **Focal Point, the DPO**, and involves continuous risk assessment, management and monitoring.

The **Focal Point** of the Group Companies has the task of enforcing this Policy in their functional areas of responsibility.

All employees/collaborators of the Group are responsible for compliance with the principles and rules defined in this document.

Compliance with the provisions of this Policy is to be considered an essential part of the contractual obligations of employees/collaborators.

Violations of this Policy may lead to disciplinary action including - in the most serious cases - dismissal, in accordance with applicable laws and national labour contracts, or termination of the collaboration relationship (for third parties).

Compliance with the provisions of the law on the protection of individuals with regard to the processing of personal data not only represents an approach in line with the principles enshrined in the Group's Code of Ethics and related documents, but also constitutes an important opportunity to rationalise, classify and order the personal data held in the company in accordance with up-to-date necessity and security criteria, limiting the duplication of excess data and avoiding the risks associated with their processing.

5.1 Definition of personal data

Personal data means **any information** relating **to an identified or identifiable natural person ('Data Subject'), either directly or indirectly, with particular reference to an identifier** such as a name, an identification number, location data, an online identifier3 or to one or more elements that are characteristic of that person's physical, physiological, genetic, psychic, economic, cultural or social identity.

6 PRIVACY ORGANISATIONAL MODEL (M.O.P.)

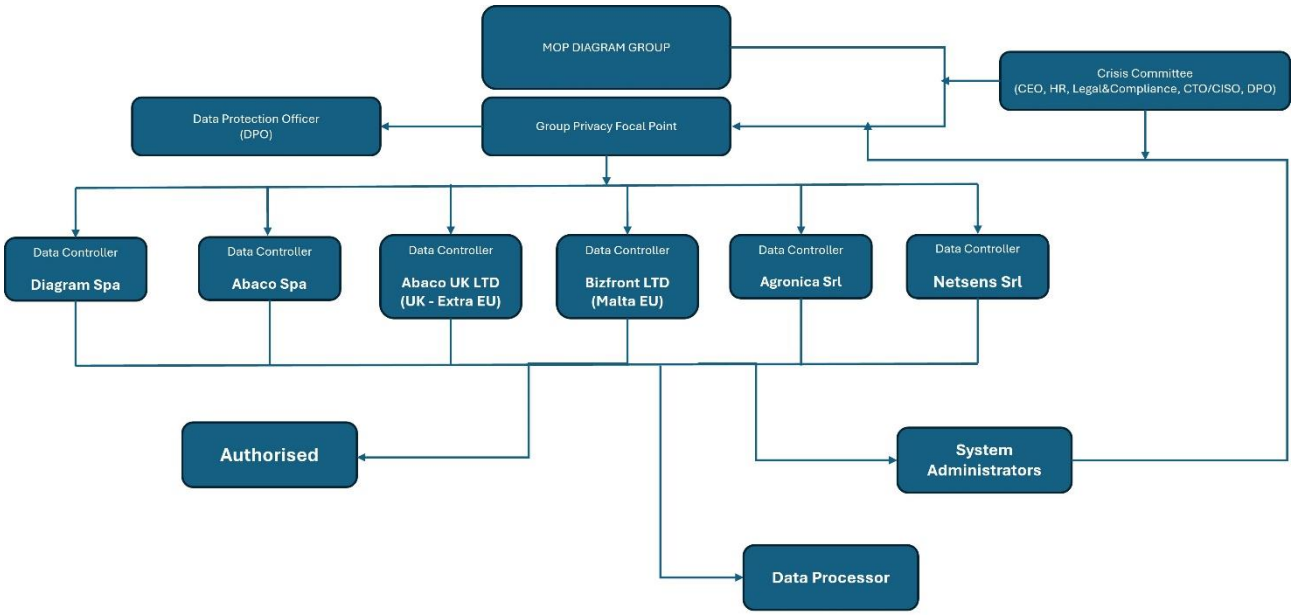
6.1 Foreword

This paragraph illustrates **the roles that are** defined and actively involved in the management of the **Privacy Organisational Model (O.M.P.)** within the DIAGRAM Group, and the **responsibilities** for **the** application of the Model on the various organisational structures.

The main figures involved in the management model for the processing of personal data are:

- Data Controller
- Data Processor (Group Companies and Third Parties) and possible Sub-Managers
- Data Protection Officer
- Crisis Committee
- Group Privacy Focal Point
- Authorised Processors

Below is the organisational chart:



MOP Organigram - November 2025

The MOP of the DIAGRAM Group is then declined for each subsidiary in the List of Privacy Subjects and in the List of System Administrators according to the provisions of the relative provision of the Guarantor.

6.2 Roles within the DIAGRAM Group

Taking into account the Group's *self-assessment* activity performed on the type of personal data processed, infra-group processing, organisational processes and technological safeguards, it has been deemed that - **as a general rule and with certain exceptions - the main Facility, where the Group's guidelines concerning the processing of personal data are provided, corresponds to the registered office (HQ) of the Parent Company DIGRAM S.p.A., the company identified as the "lead" for Data Protection issues.**

In fact, the principles and rules to be followed, when personal data are processed, within the Group

and independently of the fact that the data are processed at that location, are actually declined and shared at the registered office.
Although general guidelines on the processing of personal data are provided by the Parent Company, at local level, the roles and responsibilities of each Company have been defined in relation to the processing of personal data carried out within each organisation.
In particular, Group Companies may process personal data in their capacity as Data Controllers or Data Processors on the basis of specific agreements for the processing of personal data aimed at regulating - in the context of **intercompany relations** - the nature, purpose, duration of processing, type of personal data, categories of data subjects, obligations and rights of the parties.

6.3 Data Controller

The Data Controller is the natural or legal person who, individually or jointly with others, determines the purposes and means of the processing of personal data. On the basis of this definition, the Group Companies that act as Data Controllers have been identified.

Ownership **may** refer to all personal data processed by the Subsidiary (employee/collaborator data, customer and consumer data, etc.) or to a part of it (only employee/collaborator data or only customer and consumer data, etc.).

In particular, for personal data relating to the management of employees/collaborators, each Subsidiary holding the employment relationship is the Data Controller, while for personal data relating to customers and consumers, the Subsidiaries may act as Data Controller or Data Processor, as the case may be, on the basis of specific intra-group agreements.

6.4 Data Processor (Group Companies and Third Parties)

The Data Processor is the natural or legal person who processes personal data on behalf of the Data Controller.
Personal data may be processed in the name and on behalf of the Data Controller by companies appointed by the same (Group Companies or Third Parties), subject to the signing of a specific contract.

6.5 Group Companies

Within the framework of the Group organisation transposed in the M.O.P., the Subsidiaries, located both inside and outside the EU/EEA, sign as Data Processors special agreements for the processing of personal data aimed at regulating - in the context of intra-group relations - the nature, purpose, duration of the processing, type of personal data, categories of data subjects, obligations and rights of the Data Controller.

6.6 Third Parties

When processing is carried out by Third Parties, i.e. suppliers, business partners or consultants who - in their capacity as natural or legal persons - process personal data on behalf of the Controller or Processor, the performance of the processing shall be governed by a contract or other legal act binding the Third Party to the Company and regulating at least
the nature, purpose and duration of the processing;

- the type of personal data and the categories of data subjects;
- the prohibition to transfer personal data outside the EU perimeter;
- the application of appropriate security measures and procedures; the obligations and rights of the data controller.

These subjects, expressly identified as "Data Processors" with a specific deed/contract of appointment (so-called "Data Processing Agreement" or "DPA"), will have to provide sufficient guarantees in terms of specialised knowledge, reliability and resources aimed at implementing

adequate technical and organisational measures, also in terms of security, in order to ensure that the processing protects the rights of the Data Subjects.
The Data Processor may, in turn, have recourse to another responsible party (the Sub-Processor) subject to authorisation by the Controller.
In all cases, the Sub-Processor so designated by the Data Processor shall comply with the same obligations set out in the contract entered into between the Controller and the Processor.

6.7 Data Protection Officer

DIAGRAM S.p.A., in its capacity as Parent Company and "lead" company, has appointed a Data Protection Officer (DPO) for a number of subsidiaries in order to improve coordination at Group level of fulfilments, as well as to control and monitor the application of the provisions of the European Regulations and the corporate policies and procedures adopted in the field of privacy.

Taking into account the obligations provided for by local regulations and the specific activities performed, local DPOs may be appointed, who shall in any case act in close coordination with the Focal Point identified at Group level, and may be supported by the Crisis Committee set up within the Parent Company.
Any specificities or regulatory obligations will suggest, from time to time, the appointment of local DPOs.
In general, the DPO is responsible for

- promptly informing and advising the Subsidiaries - Data Controllers or Data Processors - on the processing of personal data, with the support of the Legal & Compliance Department of the Parent Company DIAGRAM S.p.A and the Focal Point;
- supporting all the Group's corporate functions in the management of issues impacting the processing of such data;
- supervising compliance with the applicable regulatory requirements;
- set up the compilation and updating of the Register of Processing Activities for the Companies of the Group, monitoring processing with the support of the Processing Authorised Persons.

These tasks are carried out by the DPO in full autonomy and independence, characteristics guaranteed by the fact that the DPO reports directly to the Parent Company's Board of Directors, to which he must send reports on specific activities carried out when necessary.

The accountability required of Group companies in the governance and control of privacy issues, as well as the risk-based approach, entail the need for risk assessments and adequate technical and organisational measures to be adopted right from the conception and design phase of each processing operation (the so-called 'Privacy by design' principle).
Each corporate function - called upon to start a new activity that may entail the processing of personal data or to manage pre-existing processing in new ways - must contact the Focal Point in advance and, where existing, the DPO for all in-depth analyses and checks on compliance aspects, risk analysis and security measures.

6.8 Privacy Focal Points of the DIAGRAM Group Companies

In order to facilitate interaction between the DPO and the Companies of the Group, a "Privacy Focal Point" (FPP) has been identified for the management of all issues and local specificities pertaining to the processing of personal data of the DIAGRAM Group.
The Focal Point Privacy is identified by the Managing Director of the Head of the Group, with the following tasks

- promptly updating the DPO, where present, on any issues, inherent to the protection of personal data, that arise within the Subsidiary in which the FPP operates, such as, for example:

- possible Data Breach;
- destruction or loss, even accidental, of personal data;
- unauthorised access to personal data;
- new projects or processing with privacy impacts;
- issues in the management of data subjects' rights;
- new Third Parties involved in the processing of personal data.

- feed and periodically update the Processing Register in cooperation with the DPO
- complete an Internal Audit activity in cooperation with the DPO

6.9 Authorised Processors

The Processing Authorised Persons, i.e. the persons authorised to carry out personal data processing operations, operate on the basis of specific written instructions provided upon hiring and then at each change of position/role in the area to which they belong, and sign the appropriate authorisation. Each Authorised Officer must limit himself/herself to processing personal data to the extent strictly necessary in connection with the performance of his/her duties and in accordance with the operational instructions received, under the direct authority of the Controller.
For the purpose of responsible management and in compliance with existing laws and regulations, Authorised Persons collecting, using and storing personal data must in their own area

- keep personal data accurate and up-to-date, from collection to destruction;
- protect personal data in such a way that it is not accessible to an indefinite number of persons or in any case to persons who are not authorised or who do not have a valid business reason for accessing the information;
- prevent unlawful or improper use of personal data where such use is not compatible
- with the purpose for which the data were collected;
- ensure the traceability and retraceability of personal data (access, modification, archiving) throughout their life cycle;
- store personal data only for the duration necessary for the indicated purpose and/or for the time stipulated by the rules and/or regulations in force, or in any case in accordance with the instructions given
- promptly report any breach of Privacy (unauthorised access to systems, loss, theft, destruction or deletion of data) not only to the IT Service, but also and promptly to the Focal Point and to the DPO where present;
- avoid storing personal data on non-password protected files and/or on external memories or laptops, the loss or theft of which could lead to a personal data breach ('Data Breach')
- as well as cooperating with the Focal Point in the compilation and periodical updating of the Processing Register.

7 REGISTER OF PROCESSING ACTIVITIES

In compliance with the provisions of the European Regulation, each Group Company that processes personal data is required to compile a Register of the processing activities carried out under its responsibility. The Register, prepared in written form, also in electronic format, must be kept at the disposal of the competent authority.
The Parent Company DIAGRAM S.p.A. has adopted a unique Group model dedicated to keeping the Register of Processing Activities performed by each Company of the Group, subdivided between the activities for which the Subsidiary is the Data Controller and the Data Processor, and in which the individual processing activities performed within the sphere of the Company's Departments and Functions, requests of data subjects, impact assessments, Data Processors and the relevant DPAs, etc. are mapped.
The Processing Register is an integral part of the system of proper management of personal data and of the M.O.P.; it is fed and updated periodically for each Group Company by the Compliance Function

in cooperation with the Focal Point and the DPO, where present, of each Subsidiary.

8 MANAGEMENT MODEL

Personal data processing operations must be carried out in a lawful, correct and transparent manner, strictly limited to what is necessary to pursue the purposes set out in the privacy policy and, in any case, compatible with such purposes.
Three phases of the personal data 'life cycle' can be identified

- Collection;
- Treatment;
- Termination of Treatment and Cancellation.

8.1 Collection

8.1.1 Purposes

The Processing of personal data (collected or received) by the Companies of the DIAGRAM Group must be carried out for the pursuit of legitimate purposes.
The personal data collected must be adequate, pertinent and limited to what is necessary for the purposes of their processing.
Some of the purposes are given below, merely by way of example:

- management of relations with customers and suppliers (natural persons);
- selection and recruitment of personnel and management of the employment relationship with them
- sending advertising material and other promotional and marketing initiatives
- direct sales activities;

8.1.2 Legal basis

Each processing of personal data requires the identification of the legal basis justifying the processing, i.e. the reason legitimising the processing of personal data.
With regard to personal data processed within the DIAGRAM Group, the legal bases for processing are:

- the consent of the data subject: when the data processing is explicitly authorised by the data subject for one or more specific purposes (e.g. to use the data subject's data for marketing purposes)
- the performance of a contract or pre-contractual provision: when the processing is necessary to fulfil a contract intended by the data subject (e.g. in order to send goods purchased by a customer, personal data such as name, surname, address, etc. must be collected)
- compliance with a legal obligation: when the data processing is imposed by a law, regulation, etc. (e.g. in order to invoice a customer for the purchase of goods, it is necessary to collect his tax data, etc.)
- legitimate interest of the Data Controller: when the processing is necessary for specific needs of the Data Controller provided, however, that the processing is not excessively invasive for the data subject (e.g. to install a video surveillance system for security purposes).

8.1.3 Consent

Consent, where necessary as a prerequisite for the lawfulness of the processing, must be expressed by means of a positive act whereby the Data Subject manifests his or her free, specific, informed and unambiguous intention to accept the processing of personal data concerning him or her, either in writing (including by electronic means, e.g. by checking a box on a website) or orally.
Silence, inactivity or pre-selection of boxes does not amount to consent.
Consent is deemed freely given if the data subject is able to make a genuinely free choice and is in a

position to refuse or withdraw consent without prejudice. Consent shall be deemed not to be freely given if:

- the performance of a contract, or the provision of a service, is dependent on the provision of consent that would not otherwise be necessary for the performance of that contract
- or if it is not possible to give separate consent for separate processing of personal data.

In fact, explicit consent must be requested, in a comprehensible and easily accessible form, for each specific purpose of processing. Where the processing has several purposes, consent must be given for each of them.

The burden of proof as to whether consent has been given lies with the Controller (and/or the Processor), who must be able to prove that the Data Subject has expressly consented to the processing of the data.

In the case of oral collection of consent (e.g. in the performance of telephone marketing activities entrusted to call centres), the operators entrusted with the task of contacting lists of names and managing the telephone interview for the purpose of promotional activities and/or the collection of information, shall expressly use the scripts specifically prepared (for the Privacy Policy and the collection of consent, and shall record, transcribe and document in writing the consent that has been given.

The consent of the Data Subjects is not required for the performance of certain processing operations, namely for

- the performance of a contract to which the Data Subject is a party or the performance of pre-contractual measures taken at his/her request
- the performance of a legal obligation to which the Controller is subject
- the pursuit of the legitimate interest of the Data Controller, provided that the
- interests or the fundamental rights and freedoms of the Data Subject.
- We mention below, merely by way of example, some of the purposes for which it is necessary to obtain specific consent:
- sending advertising material and other promotional and marketing initiatives
- profiling activities, i.e. processing aimed at analysing preferences, habits and consumption choices11
- activities concerning the processing of special categories of data, so-called special data (personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership; genetic data; biometric data; data relating to a person's health or sex life or sexual orientation), as well as the processing of personal data relating to criminal convictions and offences, where required by law.

Data subjects have the possibility to revoke, at any time, the consent previously given to the performance of certain processing operations.

In such cases, processing operations carried out by virtue of such consent must be promptly terminated, unless there is another legal ground for the processing (including, for example, fulfilment of a legal obligation; defence of a right in court; conditions of legitimate interest of the Data Controller overriding the interests, rights and fundamental freedoms of the Data Subject).

In all cases, consents and revocations must be appropriately tracked in order to be able to document any changes/changes requested by the Data Subject.

8.1.4 Execution of a contract

When the processing of personal data is necessary for the performance of a contract to which the data subject is party or for the performance of pre-contractual measures taken at his or her request, the processing of personal data may lawfully be based on the legal basis of the performance of a contract.

Since the criterion of necessity is fundamental to this legal basis, the processing of data will only be lawful where the contract cannot be fully performed without the processing of personal data (e.g. in

order to enter into a contract, the data subject's identification data must necessarily be requested). This circumstance consequently determines the impossibility of using this legal basis where the data are not necessary for the conclusion of the contract (e.g. for marketing purposes).

For processing based on this legal basis to be considered lawful, it will be necessary to prove

- the existence of the contract between the company and the data subject
- the validity of the contract itself;
- that the processing of those data provided by the data subject is objectively necessary for the performance of the contract.

It is always necessary to provide a privacy statement indicating the legal basis of the processing.

8.1.5 Fulfilment of a legal obligation

This legal basis applies when the processing of personal data is necessary for the fulfilment of obligations arising from the law.

This is the case with the processing of personal data necessary for the management of administrative and tax obligations imposed on companies in the context of labour relations (e.g. management of pay slips, etc.).

The legal obligation, however, must fulfil four conditions:

- It must be defined by European or national law of a state;
- These legal provisions must establish a mandatory obligation to process personal data, sufficiently clear and precise;
- Such provisions must at least define the purpose of the processing in question;
- This obligation must be imposed on the data controller and not on the persons concerned by the processing.

In such cases, the consent of the data subject is not required, but the privacy notice should nevertheless be provided, stating the legal basis of the processing.

8.1.6 The privacy policy

The principles of fair and transparent processing imply that the data subject must be informed of the existence of the processing and its purposes.

The Data Controller must provide the Data Subject with all information relating to the processing of personal data concerning him/her, in a concise, comprehensible and easily accessible form, in plain and clear language, in writing or by other means, including in electronic format (website).

The manner in which personal data are collected, used, accessed or otherwise processed must be transparent to the Data Subjects. In particular, the specific purposes for which personal data are processed must be explicit and legitimate and specified at the time of data collection.

The privacy notice must be provided to the Data Subject at the time of collection of the personal data or, if the data are obtained from another source, within a reasonable period of time but, at the latest, within one month. If the personal data are intended for communication with the Data Subject or another recipient, the Privacy Notice shall be provided at the latest at the time of the first communication of the data.

In the case of data collected directly from the Data Subject, the latter must be informed of any obligation to provide personal data and of the consequences of refusal to do so.

In the case of new processing operations or new ways of carrying out pre-existing processing operations, it will be the responsibility of each corporate function to contact the DPO in advance, also through the Privacy Focal Point, for all in-depth investigations and checks on compliance aspects

(legislation, risk and security analysis).

Diagram has prepared with common templates at least these disclosures, nothing prevents Diagram and its subsidiaries from preparing further disclosures:

- Candidate Information (to be provided in case of interviews for new hires)
- Employee Information (to be provided on the hiring of each new employee and at each update)
- Supplier information (to be provided at the contract stage)
- Customer information (published on the Corporate and Subsidiary websites and to be provided during the contract stage)
- Visitor Information (to be provided when accessing premises)
- SW Product Information (published on SW products/platforms developed by Diagram and Subsidiaries)
- Contact Information (published on Corporate and Affiliates' websites in the contact request form)

8.2 Processing - General principles

The processing operations performed by the Companies of the DIAGRAM Group must comply with the general principles dictated by the regulations and set forth below:

- Lawfulness***, correctness*** and transparency: data must be processed in a lawful, correct and transparent manner vis-à-vis the Data Subject
- ***Purpose limitation***: data must be collected for specified, explicit and legitimate purposes, specifically declared and described in a clear and comprehensible manner in the Information Notice, and subsequently processed in a manner that is not incompatible with such purposes. The use of the collected data for purposes other than those stated in the Information Notice is not allowed: should the Data Controller intend to further process the personal data for a purpose other than that for which they were initially collected, prior to such further processing he/she shall provide the Data Subject with a new Information Notice and, if applicable, the Data Subject shall collect a new explicit consent;
- ***Data minimisation***: data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- ***Accuracy***: data must be accurate and, if necessary, updated. All reasonable steps must be taken to rectify or erase inaccurate personal data in a timely manner;
- ***Limitation of storage***: data must be kept in a form which permits identification of the Data Subject for no longer than is necessary to achieve the purposes for which it was processed; and
- ***Integrity and confidentiality***: data must be processed in such a way as to ensure adequate security of personal data, including protection - by means of appropriate technical and organisational measures - from unauthorised or unlawful processing and from loss, destruction, alteration, unauthorised disclosure or access that could cause damage.

8.2.1 Processing by Third Parties

Processing of personal data carried out by Third Parties refers to all cases in which data belonging to Companies of the DIAGRAM Group, or for which Companies of the Group have been designated as Data Processors, are made accessible in any way, even by remote connection, to Third Parties.

In these cases, the provisions of paragraph 6.6 will apply.

8.2.2 Transfers outside the EU

With transfers of personal data outside the EU/EEA, there may be an increased risk that the Data

Subject may not be able to exercise his or her right to data protection, in particular to protect himself or herself against unlawful use and disclosure of such information.

When personal data are transferred from the EU/EEA to Data Controllers or Processors in third (non-EU/EEA) countries, the level of protection of individuals ensured in the EU by the European Regulation should not be compromised, including in cases of subsequent transfers of personal data from the third country to other third countries.

The transfer of personal data to a third country (to be understood as any case in which the data are accessible in a foreign country, even by simple remote access) may take place only for the purpose of pursuing the purpose communicated to the Data Subject at the time of collection and in accordance with the specific provisions concerning the transfer of personal data abroad.

The transfer of personal data processed or intended to be processed after transfer to a third country may take place to countries which - upon decision of the European Commission - ensure an adequate level of protection (transfer on the basis of an adequacy decision).

In the absence of an adequacy decision, and without prejudice to cases where transfer is permitted by law (including the unambiguous consent of the data subject; the necessity of the transfer for the performance of contractual/pre-contractual measures the necessity of the transfer for the exercise or defence of a right in judicial proceedings), the Data Controller must ensure that the lack of protection associated with the transfer of personal data to third countries is compensated for by adequate safeguards to protect Data Subjects, including the availability of enforceable rights of Data Subjects and effective remedies, through alternatively

- Binding Corporate Rules;
- Standard Contractual Clauses;
- model (ad hoc) contractual clauses authorised by a supervisory authority;
- Codes of Conduct: these are rules of conduct or uniform practices drawn up by various international bodies or even by individual States, intended to contribute to the correct application of the Regulation, according to sectoral specificities and the specific needs of micro, small and medium-sized enterprises.
- Certification mechanisms are forms of accreditation whereby a third party (certification body - CB) issues an attestation for the purpose of demonstrating compliance with the General Data Protection Regulation (GDPR) of the processing carried out.

8.2.3 Cookies and similar technologies

The websites of the Companies of the DIAGRAM Group may use cookies or similar technologies for profiling and marketing activities, in particular, in order to analyse or predict aspects of preferences and to provide targeted services or advertising content, to show content and to propose commercial initiatives.

Cookies, except those necessary for the normal operation of the websites, may be used with the prior consent of the persons concerned. Consent is acquired through the opening of a banner visible to users on their first visit to the site whereby they are invited to express their preferences regarding the use of cookies, the so-called cookie manager, in accordance with the relevant provisions of the Garante.

The cookie manager, in addition to allowing users to provide or deny consent for categories of cookies, also allows them to have granular information on the categories of cookies or in relation to each individual cookie such as the purpose of the cookie, duration, category (technical, analytical, marketing, profiling).

Consent, where given, is acquired lawfully (for the validity requirements of consent see section 8.1.3 on consent) and is tracked to document the data subject's choice.

8.2.4 Security

As part of the processing operations carried out, Group companies implement measures to guarantee a level of security appropriate to the risk.

In particular, personal data must be processed in such a way as to guarantee adequate security, including protection - by means of appropriate technical and organisational measures - from unauthorised or unlawful processing and from loss, destruction, modification, disclosure or unauthorised access.

Taking into account the state of the art, the costs of implementation in relation to the risks posed by the processing operations and the nature of the personal data to be protected, the following measures are implemented in particular

- physical access controls;
- restrictions to authorised personnel only for specific sensitive areas (Human Resources archive, Server Room)
- secure destruction of paper documentation containing personal data;
- secure deletion of computer media that, having been used for data processing, are intended for other use;
- pseudonymisation or encryption of personal data;
- timely restoration of availability and access to personal data in the event of a physical or technical incident;
- implementation of protection measures for the networks, systems and software with which personal data are processed;
- application of the principle of Privacy by design and by default in the design of systems and in the design of business processes and procedures;
- processes, tools and organisation to ensure timely reporting of any unlawful attempts to access personal data;
- procedures for handling breaches (Data Breach);
    - adoption of solutions for tracking activities performed on personal data;
    - adequate operational practices for regularly testing, verifying and evaluating the effectiveness of technical and organisational measures to ensure the security of processing.

8.2.5 Specific processing - Termination of Processing - Deletion and Destruction

The Group Companies concerned by the application of this Policy must:

- take all reasonable measures to delete or rectify, in a timely manner, data that are inaccurate in relation to the purposes for which they are processed;
- ensure that the period of retention of personal data is limited to the minimum necessary, in relation to the specific purposes of collection and processing.

In order to ensure that personal data are not kept longer than necessary, a time limit must be established for the termination of processing and for erasure.

The data retention period, as well as the criteria used to define this period in relation to the different processing activities reported in the Processing Register, are defined in the ISO27001 Management System instructions according to the Classification of Information or in specific policies for each Subsidiary.

In the event that a company of the Group intends to cease carrying out one or more processing operations, the personal data (in paper and electronic format) previously used in the context of these operations, subject to the aforementioned retention period and without prejudice to the fulfilment of legal obligations or purposes related to the exercise or defence of a right in court, will have to be deleted.

The DIAGRAM Group will ensure, in particular, that computer media are appropriately formatted in

the event of assignment of a PC (fixed or portable) or mobile phone to another employee, as well as, in the event of disposal of such equipment at the end of its life, secure deletion or destruction procedures to prevent the dissemination, even accidental, of data.

9 Rights of the data subject and feedback

The Data Subject has the right to access his/her personal data and to exercise this right easily, to be aware of the processing and to verify its lawfulness.

In particular, every Data Subject has the right to know and obtain communications in relation to:

- the purposes for which and the period during which the personal data are processed;
- the recipients of the personal data;
- the logic behind any automated data processing and the possible consequences of any profiling.

The Companies of the Group shall facilitate and may not refuse to comply with requests to exercise the rights of Data Subjects, unless they prove that they are unable to identify the data subject.

The data subject must be provided with the requested information without undue delay and, in any case, no later than one month from receipt of the request, unless an extension is granted - in cases permitted by law - taking into account the complexity and number of requests.

The rights of the data subject under the personal data protection legislation are set out below.

9.1 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, if so, to obtain access to and a copy of the data being processed.

9.2 Right of rectification

The Data Subject shall have the right to obtain the rectification of inaccurate personal data concerning him/her without undue delay, as well as the integration of incomplete personal data, by providing a supplementary declaration.

9.3 Right to erasure

The Data Subject has the right to obtain the deletion of personal data concerning him/her and the Controller is obliged to delete them without undue delay, if one of the following reasons exists

- the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
- the Data Subject withdraws the consent on which the processing is based and there is no other legal ground for the processing (including, for example, fulfilment of a legal obligation; defence of a right in court; legitimate interests of the Controller which override the interests, rights and fundamental freedoms of the Data Subject)
- the data subject objects to the processing of personal data concerning him/her;
- personal data are unlawfully processed.

9.4 Right to restriction of processing

The Data Subject has the right to obtain the restriction of processing when, among other cases

- he/she disputes the accuracy of the personal data, for the period necessary for the Controller to verify the accuracy of such data;
- when, in the face of unlawful processing, the Data Subject objects to the deletion of personal data and requests instead that their use be restricted.

Ways of restricting the processing of personal data may include temporarily transferring the selected data to another processing system, or making the selected personal data inaccessible to users, or

temporarily removing the published data from a website.

9.5 Right to data portability

The Data Subject has the right to receive, in a structured, commonly used and machine-readable format, the personal data concerning him/her that he/she has provided and to transmit it to another Data Controller without hindrance, if:

- the processing is based on consent or if the processing is necessary for the performance of a contract
- to which the Data Subject is party; and
- the processing is carried out by automated means.

When exercising his or her data portability rights, the Data Subject has the right to obtain the direct transmission of personal data from one Data Controller to another, if technically feasible.

Where a certain set of personal data concerns more than one data subject, the right to data portability must not affect the rights and freedoms of other data subjects.

9.6 Right to object

The data subject has the right to object at any time to the processing of personal data concerning him or her.

The exercise of this right results in the abstention from further processing of personal data, unless it can be demonstrated that there are compelling legitimate grounds for processing which override the interests, rights and freedoms of the Data Subject or for the establishment, exercise or defence of legal claims.

If personal data are processed for direct marketing purposes, the Data Subject has the right to object - at any time and free of charge - to such processing, including profiling related to direct marketing purposes.

9.7 Reply to the applicant and time limits

Before responding to the exercise of rights, it is essential that Group Companies take all reasonable steps to verify the identity of the Data Subject, or of the person making the request on their behalf, particularly in the context of online services or online identifiers, by requesting - where appropriate - a copy of a valid identity document.

If the request comes from a person acting on behalf of the data subject, it is necessary to verify

- the proxy signed by the data subject;
- the identity of the data subject and of the delegated person.

If the request concerns access to the data of a deceased person, it is necessary to identify the requester and make sure that he is an heir, or in any case, a person entitled to exercise the right. The reply given to the data subject or to the person delegated by him/her should be traced.

If requests are addressed directly to the Customer Service, it will be the Customer Service's task to check the history of the data processed (collection, use, archiving, deletion), to execute the requests of the Interested Parties and to confirm to them the outcome of the requests.

Where doubts arise in the interpretation of the requests received, in strict compliance with the response times provided for by the law, it is advisable for the Customer Service Manager to involve the Focal Point and, where possible, the DPO in order to agree on and define the correct action to be taken.

Only in the case of requests addressed directly by the Data Subjects to the DPO through the dedicated channel (e-mail address DPO@diagramgroup.it), the latter will involve the Focal Point and the Customer Service for the necessary verifications and authorise the appropriate actions, giving direct

confirmation to the Data Subjects.

The requests of the Interested Parties will be recorded from time to time by the affiliates that received them in a special register.

10 Operating Instructions

Each Company of the DIAGRAM Group, in order to deal with requests that may be received from the Interested Parties, in particular from customers and/or consumers, with regard to the above-mentioned rights, makes known to the Interested Parties, on the institutional websites of the Companies of the Group, the e-mail address of the DPO (DPO@diagramgroup.it) where present and of the Focal Point (privacy@diagramgroup.it), as well as the Contact Centre for customer support activities.

11 Privacy by design & by default

The principle of accountability entails being able to demonstrate compliance with the European Regulation through the adoption - right from the conception and design phase of the personal data processing activity ("Privacy by design") - of appropriate technical and organisational measures and internal policies to ensure that only the personal data necessary (in terms of quantity, scope of processing, retention period and accessibility) for each specific processing purpose are processed by default ("Privacy by default").

These measures consist, inter alia, of minimising the processing of personal data, pseudonymising personal data as quickly as possible, enabling data subjects to control the processing of their data, creating and improving security features, and defining clear internal divisions of responsibility.

With the ultimate aim of implementing solutions for the design of personal data processing, processes and information systems capable of protecting data during all phases of the 'life cycle', the DIAGRAM Group implements technical and organisational measures to preventively guarantee the protection of processed data, ensuring compliance with the following principles

- Responsibility in data processing on the part of all the Group's collaborators and business partners, in order to safeguard the confidentiality, integrity and availability of the personal data processed;
- information to Data Subjects on the manner in which DIAGRAM collects, uses, stores and communicates personal data;
- Use and storage of data exclusively for the purposes declared to the Interested Parties and expressly authorized by their consent;
- transfer of data to business partners only for the purposes identified in the information notice and with a
- adequate level of security;
- limited access to data by authorised personnel trained in handling personal data;
- monitoring of the correct application, both internally and externally, of the principles and indications provided in this Policy.

The Privacy by Design and by Default approach must consider the entire 'lifecycle' of personal data, from collection to deletion, taking due account of any data processing operation (recording, storage, consultation, use, communication, transfer) and safeguarding its confidentiality, integrity and availability, in all processes/systems/applications through which personal data are processed.

These principles must be integrated into the Group's entire organisation: each company function called upon to start a new activity that may involve the processing of personal data or to manage pre-existing processing in new ways, must contact the DPO and the Focal Point in advance for all in-depth analyses and checks on compliance aspects (regulatory, risk analysis and security).

The IT model used by the DIAGRAM Group for mapping data processing makes it possible to assess the possible risks arising from the design of a new processing operation and to carry out a Data Protection

Impact Assessment (DPIA), if necessary, in order to make the necessary corrections.

12 Data Protection Impact Assessment (DPIA)

In the event that a type of processing, in particular if it involves the use of new technologies or if it is of new application, presents a high risk for the rights and freedoms of the Data Subjects, the Companies of the Group, before proceeding with the processing itself, carry out an impact assessment on the protection of personal data, aimed at determining in particular the likelihood and seriousness of such risk taking into account the nature, scope, context and purpose of the processing.

The outcome of the assessment must be taken into account in determining the appropriate measures and safeguards to be adopted to mitigate the risk and to comply with the provisions of the Regulation.

Where such measures are not feasible, in view of the technology available or the costs of implementation, the supervisory authority must be consulted before processing activities commence.

The impact assessment must be updated, with the assistance of the DPO and the support of the Focal Point, periodically or whenever it proves necessary in the light of the time elapsed since the initial processing or whenever there are significant changes in the processing in the type of data processed, in the processing methods, in the technological solutions employed that may have significantly altered the initial analysis.
The assessment takes into account the entire 'life cycle' of personal data, from collection to deletion and takes into account any specific elements required by the particular context in which the processing takes place (e.g. direct marketing, profiling, children's data, etc.) as well as applicable legislation.

13 Data Transfer Impact Assessment (TIA)

In the event that the processed personal data are to be transferred to Group Companies or to Third Parties located in countries outside the EU/EEA that do not offer an adequate level of protection or protection equivalent to that provided by the GDPR, before processing, an impact assessment on the transfer of personal data (Transfer Impact Assesment or 'TIA') must be carried out in order to assess the legislation in force in the country of transfer and the risks and seriousness of the same for the rights and freedoms of the data subjects, taking into account the nature, scope, context and purpose of the processing.

Group companies affected by the need to prepare the TIA are required to document the transfer impact assessment process and, where requested, to make it available to the competent supervisory authority.

The outcome of the assessment will have to be taken into account in determining the further measures and safeguards to be adopted for risk mitigation and compliance with the provisions of the Regulation.

14 Data Breach Notification

A personal data breach (Data Breach) may, if not addressed in an appropriate and timely manner, result in harm to Data Subjects, such as: loss of control over personal data concerning them or limitation of their rights; discrimination, identity theft or usurpation; financial loss; damage to reputation; loss of confidentiality of personal data protected by professional secrecy; or any other significant economic or social harm to the natural person concerned.

Therefore, in cases of violation of personal data, the Company of the DIAGRAM Group that has suffered the violation must

- verify that all appropriate technological and organisational protection measures have been put in place according to the breach;
- promptly inform the Data Controller, the Focal Point and the DPO, if any, within 24 hours, so that the competent supervisory authority can be notified of the event without undue delay and, where possible, within 72 hours of becoming aware of it.

The DIAGRAM Group has defined and issued, with the support of the DPO, the Data Breach Procedure for the correct management of security incidents relating to personal data, which is referred to in full as regards the operating methods envisaged by the said procedure.

By way of example and without limitation, possible data breach events may consist of

- **irretrievable loss of data** (whether in electronic or paper format) understood as the ascertained impossibility of restoring them. By way of example: cases of loss/theft of computer media or events of fire/flooding of paper archives;
- **unauthorised access to data** (computer systems or paper archives) understood as a violation of the confidentiality of the data contained in the same systems or archives. By way of example: a computer attack by exploiting vulnerabilities in the systems or abusive use of authentication credentials; consultation of paper archives to which access is defined as restricted to authorised personnel only;
- **loss of data integrity** in **the** sense of irreparable impairment of the correctness, congruence and consistency of the data. By way of example: compromise resulting from unauthorised modification of data, human error, computer incidents;
- **revelation or disclosure of data** (whether in electronic or paper format) to unauthorised third parties, even unidentified ones, e.g. by e-mail or even verbally.

Any situation of personal data violation must be promptly reported by those who become aware of it:

- for DIAGRAM S.p.A., to the Focal Point, to the DPO if present, to IT Department and to the Legal&Compliance department;
- for all other Subsidiaries, to the Focal Point ; it will be the responsibility of the Focal Point to inform the local DPO (if present) and the Group DPO (if present), the IT department and the Legal&Compliance department promptly, and in any case within 24 hours.

Once the report has been received, the DPO and the Focal Point will immediately inform the Data Controller and proceed to assess the anomaly.

Only in the event that the event is actually deemed to be a Data Breach, the Data Controller will take note of the necessary corrective measures (Data Breach mitigation activities) and, unless the breach is unlikely to present a risk for the rights and freedoms of the Data Subjects, will notify the ascertained breach to the competent supervisory authority, without undue delay and, where possible, within 72 hours from the time it came to its knowledge.

If the breach exposes the Data Subjects to high risks, the Controller will, without undue delay, send a direct communication to each of them, describing the nature of the breach ascertained.

15 Inspections by the Supervisory Authority

The competent supervisory authorities may carry out inspections at the companies of the DIAGRAM Group aimed at verifying their effective application of the provisions of the law.

During such inspections, the Group will adopt the precautions and safeguards envisaged by the internal regulations concerning relations with the public supervisory authorities.

In general, in the event of contact with officials representing the offices of the supervisory authority, the Focal Point and the DPO must be notified immediately.

Documents or information related to the processing of personal data may only be handed over to inspectors with the authorisation of a representative of the Legal&Compliance Office, who must attend the inspection visit.

The Parent Company DIAGRAM S.p.A., is entrusted with acting as a point of contact with the Authority for the Protection of Personal Data for matters related to processing, facilitating the Authority's access to the necessary information and cooperating with it.

16 Rules of conduct in case of inspection activities

All personnel, howsoever involved in the management of inspection visits by the Control Authority, are required to observe the rules of conduct indicated by the Company where they work, as well as the relevant Policies and Procedures.

Reference is made in full to the operating methods set out in the procedure for the Management of Inspections of the Quality Management Systems of each subsidiary.

As a general rule, it is recommended to adopt a collaborative attitude with the Control Authority: the duty to collaborate implies the obligation to allow access to documents, both on paper and in electronic format contained in computers, hard disks and in any other IT device, the obligation to indicate where the documents of interest are kept, as well as the obligation to provide any information requested regardless of the fact that the documents or information are kept in different places or by parties other than the Group Companies, Data Controllers or Processors, (such as Third Party Processors).

Answers to questions asked by inspectors should refer as far as possible to the procedures adopted and the personal data processing carried out, so as to avoid generic answers, reserving the right - in case of uncertainty - to provide clarifications and/or answers as well as more detailed documentation at a later stage.

17 Training

The privacy training plan (courses, recipients, timing) is defined, at Group level, at the initiative of the Data Controller, by the HR and Legal&Compliance Functions of the Parent Company in coordination with the DPO and the Focal Point.

The purpose of the training is to train and inform persons authorised to process data on

- legislative frameworks, compliance with regulations and the provisions of the Privacy Guarantor;
- type of data and processing methods;
- the Privacy management model implemented;
- roles envisaged for the processing of personal data;
- information and consent, access rights, complaints and sanctions;
- the security measures adopted.

In cases of new hirings, job changes or the introduction of new significant tools relevant to the processing of personal data, the HR Function - with the support of the Focal Point - is responsible for ensuring that the training plan is updated and delivered in a reasonably short time.

18 Audit

The Group Legal&Compliance Function, within the scope of the activities envisaged in the Audit plan, may carry out assurance activities on the level of compliance with the rules set out in this document and with the reference regulatory framework, starting from the results of any audits conducted by the DPO or by specifically appointed persons, reserving the right, if necessary, to carry out in-depth and/or additional ad hoc audits.

Audit activities may also be extended to Third Parties (suppliers) operating in the name and on behalf of individual Group companies.

19 Sanctions

Violation of the regulations on the protection of personal data may expose the Companies of the Group to various types of responsibilities and consequent sanctions (of an administrative and/or penal nature) depending on the regulations concretely violated and may have a significant negative reputational impact on the DIAGRAM Group, even significant.

Failure to comply with the obligations envisaged by this Policy constitutes conduct that is relevant for

disciplinary purposes and may lead to the application of the disciplinary sanctions envisaged by current laws and national labour contracts.