PERSONAL DATA PROCESSING SECURITY POLICY OF THE COMPANY ASCENDIS CONSULTING S.R.L..

ASCENDIS CONSULTING S.R.L

PERSONAL DATA PROCESSING SECURITY POLICY OF THE COMPANY ASCENDIS CONSULTING S.R.L.

This security policy was created taking into account the following:

- The fact that **ASCENDIS CONSULTING S.R.L**., with its registered office in Bucharest, 2B Ion Ionescu de la Brad Street, sector 1, registered with the Trade Register Office under no. J40/3140/97, unique registration code RO 9398288, having the bank account no. RO20RZBR0000060005322908, opened with Raiffeisen Moşilor Branch, represented by Andrei GOŞU, Manager (hereinafter referred to as "**Ascendis**" or "**We**") carries out an activity that involves the processing of certain categories of personal data.,

- the entry into force starting with May 25, 2018, of the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, On the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC. (hereinafter referred to as the "**GDPR**"),

- the obligation imposed by the GDPR to provide technical and organizational security measures appropriate to all personal data processing activities.

1. UNDERTAKING

Ascendis processes personal data for legitimate purposes, in compliance with all the principles imposed by GDPR and ethical commercial practices. Protecting the safety and security of personal data is important for Ascendis and this policy describes the organizational framework implemented in order to ensure processing compliance.
The main objective of this Security Policy is to contribute to the development of the company's activity in compliance with the specific legal provisions and to minimize risks by preventing incidents and, in the unlikely event of such incidents, reducing their impact on the data subject.
We aim at having a relationship based on trust, transparency, good faith and ethics in relation to all our partners, collaborators and employees.

2. DEFINITIONS

'Personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

'Processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
'Pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.
'Controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.
'Processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
'Third party' means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorized to process personal data.
'Recipient' means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing.
'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.
'Restriction of processing' means the marking of stored personal data with the aim of limiting their processing in the future.

3. THE PRINCIPLES OF THE SECURITY POLICY

Ascendis processes the personal data that comes in contact with in compliance with the following principles:

- **Protection of the fundamental rights and freedoms** of the data subjects;

- **Lawfulness, fairness and transparency -** personal data are processed in good faith and in accordance with the legal provisions in force, in a fair and transparent way in relation to the data subject;

- **Determined, explicit and legitimate purposes -** The processing of personal data by Ascendis is made for determined, explicit and legitimate purposes and they are not subsequently processed in a way incompatible with these purposes;

- **Legal basis -** Ascendis will ensure that any processing of personal data will have a well-defined basis, such as legal provisions, the consent of the data subject, the execution of contracts, the legitimate interest of Ascendis (which will not contravene the best interests of the data subject);

- **Purpose limitation -** Ascendis processes personal data only if they are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

- **Time limitation** - Ascendis keeps the data of the data subjects for a period that does not exceed the **period necessary to fulfill the purposes for which the data are processed**;

- **Accuracy -** Ascendis processes personal data in a precise manner and takes reasonable measures to ensure that the inaccurate data it becomes aware of are deleted or rectified;

- **Security -** Ascendis is committed to ensuring the security of all personal data that it processes and makes constant efforts to achieve this purpose, including by training its employees, collaborators and partners.

4. CATEGORIES OF DATA SUBJECTS

Ascendis processes the personal data of the following categories of data subjects:

- Employees and own collaborators;
- The employees of commercial partners;
- as the case may be, other natural persons interacting with the company during its activity.

5. DATA COLLECTED

Depending on the specificity of each relationship, Ascendis can process the following categories of data regarding the data subjects:

- Surname and name;
- Contact details: telephone, e-mail address;
- Identification data, according to the identity card / passport;

- Professional data: job, position, seniority, professional experience;
- Data provided directly by e-mail or other means by the data subjects;
- Data collected about employees and their families or employees, in order to comply with the employment/collaboration contract and the legal provisions in the labor field;
- Psychological profiles of the clients' employees made at the clients' request and with the acceptance of the data subjects.

The personal data mentioned above are examples.
This data can be collected from the following **sources**:

- From Ascendis's clients;
- from contracts and ancillary documents , including in the execution of work/collaboration relationships;
- as a result of them being supplied directly by the data subject - with obtaining the consent in the cases provided by law;
- as a result of the interaction of our employees/collaborators with the data subjects (e.g. business cards, attendance lists at events));
- from public sources;

6. PURPOSES AND BASIS FOR PROCESSING

Ascendis is the largest training and consulting company in the field of organizational development in Romania. The processes of organizational transformation that our clients go through are always measured by concrete results. And this is not a mere statement of intent, but our business philosophy, implemented through modern know-how, by experienced consultants. The requirements of our partners are diverse and complex. Some are related to the development of skills or attitudes for employees. Others are related to strategy, processes and concrete implementation ability. Regardless of the requirement, our interventions combine modern learning methodologies and tools: microlearning, experiential, gamification, coaching, business simulations or mentoring, to name a few of them.
Thus, we collect personal data for the following **purposes**:

a) provision of training and organizational consulting to our clients, legal persons, for their staff;
b) Promotion of Ascendis group's products and services;
c) Execution of contracts with suppliers and partners;
d) In the process of recruiting and managing our employees/collaborators, or occasionally for clients;

We collect personal data on the following **bases**:

a) Execution of contracts. Our company offers services almost exclusively to legal persons, thus processing personal data in the execution of contracts with them;

b) The consent of the data subjects. In some cases, the consent will be considered granted by the fact that the data subject will have the initiative of transmitting personal data to us, for example, in case of contacting the company on his/her own initiative by the data subject through the email address of Ascendis;
c) Fulfillment of legal obligations;
d) Fulfillment of the legitimate interests of Ascendis that will not oppose the superior rights of the data subject.

7. RECIPIENTS

Some of our partners are located outside the European Union. We provide our clients integrated services which also involve a transfer of personal data to these partners.
Below are our partners from outside the European Union with whom we collaborate in order to provide the Ascendis services:

A) Blue EQ, with an innovative approach, BlueEQ is the creator of the most modern and practical development tool for the development of Emotional Intelligence for individuals and teams. Ascendis has been representing BlueEQ in Europe and the Middle East since 2016.
B) Harrison Assessments, world leader in the research, design and publication of valid psychometric instruments that measure effectiveness at individual, group and organizational level.
C) Society for Human Resources Management, an Association dedicated to human resources management and HR Certification Institute, the world leader in the field of examination of human resources professionals.
D) International Association for Six Sigma Certification, the only independent international association that can certify Lean Six Sigma specialists.

Ascendis and its non-EU partners want to comply with the GDPR and ensure a high degree of protection of personal data. In addition to the technical security measures implemented by our partners, there is an appropriate documentation consisting of type-contractual clauses that ensure an adequate level of protection.
Ascendis does not sell, offer or make available the personal data they process to third parties in commercial interest.
Also, personal data can be transmitted to the public authorities, according to the law (for example, to the Ministry of Education), as well as to our contractual partners with whom we collaborate to provide services to our clients and who ensure that they will implement appropriate measures regarding the security of personal data.
The data of the data subjects can be stored in a database in the European Union (EU) or outside the EU, in compliance with the security guarantees mentioned above. Ascendis undertakes to ensure the confidentiality of the personal information processed. Ascendis, directly or through its authorized agents, will process the data as a personal data controller, and these data can be accessed and used only by other companies in the Ascendis group, directly or through their authorized agents, as well

as by the contractual partners of the controller, directly or through its authorized agents.
If Ascendis is required to disclose the information of the data subjects by a court order or to comply with other legal or regulatory requirements, the company will respond to these requests in accordance with the legal provisions in force..

8. THE RIGHTS OF THE DATA SUBJECTS

According to the GDPR, all natural persons to whom we process personal data have specific rights, among which we mention:

a) **Right to be informed:** the right to find out what data are being processed, the purposes and grounds of the processing, the recipients of the data, the storage period, the existence of the rights of the data subjects, the right to address the supervisory authority, etc..;

b) **Right of access:** the right to obtain from the controller a confirmation whether or not personal data concerning them are processed and, if so, access to the data and processing information previously detailed;

c) **Right to rectification**: the right to obtain the correction of inaccurate data or to complete the missing data;

d) **Right to data erasure:** the right to request the erasure of the processed data, in the situations provided by law;

e) **Right to restrict processing**, within the limits stipulated by the law.

f) **Other rights** that can be exercised within the limits provided by law: the right to data portability, the right to object to data processing, the right to oppose automatic decision-making processes, the right to address the competent authorities with requests regarding the processing performed by Ascendis etc..

9. SECURITY OF DATA COLLECTED

In accordance with the legal provisions in force and the current status of the technology, Ascendis has implemented adequate technical and organizational measures in order to ensure the security of personal data during our activity, according to the rules detailed below.
In our activity, we aim first and foremost at preventing any security incidents, such as unauthorized access to data, data leaks, accidental deletion of data and the like, the entire structure of data processing being built around the principle of prevention.

However, considering that in the information society, the security of the processing cannot be 100% guaranteed; Ascendis has also taken measures so that, in the unlikely event that security incidents occur, their extent and severity are diminished.
Given that some of the information collected may be sensitive (for example, the professional profiles and those regarding the preferences of the employees of our clients about whom we are required to make such profiles), we assume the imposition of additional security standards for this information.

10. GENERAL RULES

To ensure adequate protection of the personal data to which Ascendis has access, we have implemented organizational and technical measures, such as:

a) Signing of additional documents with our employees, collaborators and partners in order to ensure the confidentiality of personal data to which they have access at least to a level similar to that imposed by our company.

b) Implementation of physical security measures regarding documents that contain personal data, such as, for example, storing documents in locked cabinets with access to only authorized personnel, implementation of restricted access systems (for example , keys, access cards) exclusively for persons who justify an interest in accessing the respective data.

c) Implementation of security measures regarding computer systems, such as, for example, the assurance that all our equipment has appropriate security programs, ensuring backups, etc.

d) Implementation of training programs for personnel regarding GDPR requirements.

11. SPECIFIC RULES

Ascendis has implemented the following specific rules for the protection of personal data:

a) **Technical Security Rules**

i. Prohibiting the use by users of systems of unlicensed software or from uncertain sources;

ii. Implementation of a user-based authentication system and secure passwords, unique to each authorized user; thus, on the one hand it is prevented the access of third parties to the terminals/databases and, on the other hand, upon the incorrect entry of the username password a certain

number of times, the system locks automatically, according to the internal technical procedures;

iii. Implementation of adequate security measures of the IT equipment and software used in our activity, as follows:

- informing users about the danger regarding computer viruses;
- implementation of appropriate protection software on the terminals used, such as antivirus programs and informing the employees about the obligation to periodically scan the systems in order to prevent any unauthorized programs (e.g. malware, phishing) or, as the case may be, the implementation of automatic virus removal and security of information systems;
- deactivating as much as possible the "Print screen" key, when personal data are displayed on the monitor, thus limiting the possibility to print them by users other than those authorized in this regard;
- limitation of printing rights, by implementing systems based on user/password;
- monitoring access to the database and access login and path of the user;
- periodic change of passwords for access to databases and information systems;
- the obligation of the employees to secure the access in their own terminals when they do not use them and to close the terminals at the end of the work program;
- limiting access rights to remote databases (i.e. from outside the company)/using other devices than those made available by the company.

b) **Organizational Security Rules**

i. Limiting the number of recipients / users who have access to personal data and correlating access rights with the need justified by each user - e.g. by dividing the information about the data subjects on geographical areas, by transmitting to the processors only the data necessary for the execution of the contract, etc.;

ii. Implementation of conditions and obligations of confidentiality and protection of additional personal data for employees, collaborators, suppliers and partners;

iii. Implementation of specific rules on copying and disseminating documents in order to prevent the spread and access of unauthorized persons to personal data;

iv. Implementation of rules by which our employees, collaborators and partners have access only to those personal data necessary to fulfill the job description or, as the case may be, the obligations assumed towards Ascendis;

v. Installation of alarm systems and access monitoring in the spaces where the documents containing personal data are stored or where the equipment on which these data are stored are by the owner of the building in which we carry out our activity;

vi. Installation of systems to ensure the physical security of documents that include personal data, such as locked cabinet with a key, to ensure video surveillance of the building in which we carry out our activity (the video supervised areas being appropriately marked) by the owner of the building in which we carry out our activity;

vii. Creation of backups of stored data;

viii. Unauthorized persons access restriction in the areas where personal data are stored or where the equipment on which they are stored, except with the provision of appropriate confidentiality conditions;

ix. Prohibiting the copying of personal data on mobile storage media, without the prior agreement of the company's management, except the situation when it is necessary to fulfill contractually assumed obligations towards customers;

x. Ensuring the periodic training of personnel regarding the GDPR requirements, as well as on the security and risks regarding personal data.

12. FINAL PROVISIONS

For more details, information and requests, any interested person can send an e-mail to the dedicated address anca.barbu@ascendis.ro, by phone to the number 0212066429 or directly to our headquarters in Bucharest, 2B Ion Ionescu de la Brad Street, sector 1. For the exercise of certain rights, we reserve the right to request that the application be filed in writing, signed by the data subject and that the applicant to

present sufficient evidence of identification with the data subject (who exercises the right conferred by law).