# Data controller agreement

Insertion of standard contractual clauses pursuant to art. 28.7 GDPR

## TYPE CONTRACTUAL CLAUSES

These clauses were inserted with the Commission Implementing Decision (EU) 2021/915 of 4 June 2021 pursuant to Article 28, paragraph 7, of Regulation (EU) 2016/679 of the European Parliament and of the Council in order to be used in contracts between a data controller and a controller who processes personal data on behalf of the data controller.

## SECTION I.

### *Clause 1 - Purpose and scope of application*

a) The purpose of these standard contractual clauses (hereinafter "clauses") is to ensure compliance with Article 28, paragraphs 3 and 4, of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data, as well as the free circulation of such data and which repeals Directive 95/46 / EC (General Data Protection Regulation, or GDPR).

b) The data controllers and data processors referred to in Annex I have accepted these clauses in order to ensure compliance with Article 28, paragraphs 3 and 4, of Regulation (EU) 2016/679.

c) These clauses apply to the processing of personal data specified in Annex II.

d) Annexes I to IV form an integral part of the clauses.

e) These clauses are without prejudice to the obligations to which the data controller is subject in accordance with Regulation (EU) 2016/679.

f) These clauses do not, in themselves, guarantee compliance with the obligations related to international transfers in accordance with Chapter V of Regulation (EU) 2016/679.

### *Clause 2 - Invariability of the clauses*

a) The parties undertake not to modify the clauses except to add or update information in the attachments.

b) This does not prevent the parties from including the standard contractual clauses set out in these clauses in a broader contract or from adding other additional clauses or guarantees, provided that these do not directly or indirectly contradict these clauses or harm any rights or freedoms fundamentals of the data subjects.

### *Clause 3 - Interpretation*

a) When these clauses use the terms defined in Regulation (EU) 2016/679, these terms have the same meaning as in the regulation concerned.

b) These clauses must be read and interpreted in light of the provisions of Regulation (EU) 2016/679.

c) These clauses must not be interpreted in a sense that does not comply with the rights and obligations provided for by Regulation (EU) 2016/679, or that prejudices the fundamental rights or freedoms of the data subjects.

## *Clause 4 - Hierarchy*

a) In case of contradiction between these clauses and the provisions of related agreements, in force between the parties at the time of acceptance of these clauses, or concluded subsequently, these clauses prevail.

## *Clause 5 - Subsequent accession clause*

b) Any entity that is not a party to these clauses may, with the agreement of all parties, adhere to these clauses at any time, as data controller or data processor, by completing the attachments and signing the attachment THE.

c) Once the annexes referred to in letter a) have been completed and signed, the adhering entity is considered a party to these clauses and has the rights and obligations of a data controller or data processor, in accordance with its designation in the Annex I.

d) The Participating Entity has no rights or obligations arising under these clauses for the period prior to membership.

# SECTION II - OBLIGATIONS OF THE PARTIES

## *Clause 6 - Description of the treatment*

The details of the processing, in particular the categories of personal data and the purposes of the processing for which the personal data are processed on behalf of the data controller, are specified in Annex II.

## *Clause 7 - Obligations of the parties*

*7.1. Instructions*

g) The controller processes personal data only on the documented instruction of the controller, unless required by Union or national law to which the controller is subject. In this case, the data controller informs the data controller about this legal obligation before processing, unless the law prohibits it for relevant reasons of public interest. The data controller may also give subsequent instructions for the entire duration of the processing of personal data. These instructions are always documented.

h) The data controller immediately informs the data controller if, in his opinion, the instructions of the data controller violate Regulation (EU) 2016/679 or applicable national or Union provisions relating to data protection.

*7.2. Purpose limitation*

The data controller processes personal data only for the specific purposes of the processing referred to in Annex II, unless further instructions from the data controller.

*7.3. Duration of the processing of personal data*

The controller processes personal data only for the duration specified in Annex II.

*7.4. Security of treatment*

a) The controller shall implement at least the technical and organizational measures specified in Annex III to ensure the security of personal data. This includes protection from any security breach that accidentally or unlawfully results in the destruction, loss, modification, unauthorized disclosure or access to data (personal data breach). In assessing the adequate level of security, the parties take due account of the state of the art, the implementation costs, as well as the nature, scope, context and purpose of the processing, as well as the risks for the data subjects. .

b) The controller grants access to the personal data being processed to its staff members only to the extent strictly necessary for the implementation, management and control of the contract. The data controller guarantees that the persons authorized to process the personal data received are committed to confidentiality or have an adequate legal obligation of confidentiality.

*7.5. Sensitive data*

If the processing concerns personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, genetic data or biometric data intended to uniquely identify a natural person, health data or to the sexual life or sexual orientation of the person, or data relating to criminal convictions and offenses ("sensitive data"), the controller applies specific limitations and / or additional guarantees.

*7.6. Documentation and respect*

d) The parties must be able to demonstrate compliance with these clauses.

e) The data controller responds promptly and adequately to the data controller's requests for information regarding the processing of data in accordance with these clauses.

f) The data controller makes available to the data controller all the information necessary to demonstrate compliance with the obligations established in these clauses and which derive directly from Regulation (EU) 2016/679. At the request of the data controller, the data controller allows and contributes to the review activities of the processing activities referred to in these clauses, at reasonable intervals or if there are indications of non-compliance. When deciding on a review or review activity, the controller may take into account the relevant certifications held by the controller.

g) The data controller may choose to conduct the audit independently or appoint an independent auditor. Audit activities may also include inspections of the controller's physical premises or facilities and, where appropriate, are carried out with reasonable notice.

h) Upon request, the parties shall make available to the competent supervisory authority or authorities the information referred to in this clause, including the results of any audit activities.

*7.7. Recourse to sub-processors*

a) The data controller has the general authorization of the data controller to use sub-processors d and processing on the basis of an agreed list. The data controller specifically informs the data controller in writing of any planned changes to this list regarding the addition or replacement of sub-processors at least one (1) month in advance, thus giving the data controller time. sufficient to be able to object to such changes before recourse to the sub-processor or sub-processors in question. The data controller provides the data controller with the information necessary to allow him to exercise the right to object.

b) If the controller uses a sub-controller for the performance of specific processing activities (on behalf of the controller), he enters into a contract which essentially requires the sub-controller to do the same data protection obligations imposed on the controller in accordance with these clauses. The data controller ensures that the sub-processor complies with the obligations to which the data controller is subject pursuant to these clauses and Regulation (EU) 2016/679.

c) At the request of the data controller, the data controller provides him with a copy of the contract stipulated with the sub-processor and any subsequent changes. To the extent necessary to protect business secrets or other confidential information, including personal data, the controller may remove information from the contract before transmitting a copy.

d) The data controller remains fully responsible towards the data controller for the fulfilment of the obligations of the sub-processor deriving from the contract he has entered into with the data controller. The data controller notifies the data controller of any non-fulfilment by the sub-processor of contractual obligations.

e) The controller agrees with the sub-processor a third beneficiary clause according to which, if the controller has effectively disappeared, has legally ceased to exist or has become insolvent, the controller has the right to terminate the contract with the sub-processor and require the latter to delete or return the personal data.

*7.8. International transfers*

a) Any transfer of data to a third country or an international organization by the controller is carried out only on the documented instruction of the controller or to fulfill a specific requirement under Union or Member State law to which the data controller is the subject, and in compliance with chapter V of Regulation (EU) 2016/679.

b) The data controller agrees that, if the data controller uses a sub-processor in accordance with clause 7.7 for the performance of specific processing activities (on behalf of the data controller) and such processing activities involve the transfer of personal data pursuant to chapter V of Regulation (EU) 2016/679, the data controller and the sub-processor can guarantee compliance with chapter V of Regulation (EU) 2016/679 using the standard contractual clauses adopted by the Commission in accordance with Article 46 (2) of Regulation (EU) 2016/679, provided that the conditions for the use of such standard contractual clauses are met.

## *Clause 8 Assistance to the data controller*

a) The data controller promptly notifies the data controller of any request received from the data subject. He does not respond to the request himself, unless authorized to do so by the data controller.

b) The data controller assists the data controller in fulfilling the obligations to respond to requests from data subjects for the exercise of their rights, taking into account the nature of the processing. In fulfilling the obligations referred to in letters a) and b), the data controller follows the instructions of the data controller.

c) In addition to the obligation to assist the data controller in accordance with clause 8, letter b), the data controller also assists the data controller in ensuring compliance with the following obligations, taking into account the nature of the data processing and information available to the data controller:

1. the obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data ("data protection impact assessment") if a type of processing may present a high risk for the rights and freedoms of individuals physical;

2. the obligation, before proceeding with the processing, to consult the competent supervisory authority or authorities if the data protection impact assessment indicates that the processing would present a high risk in the absence of measures taken by the data controller to mitigate the risk;

3. the obligation to ensure that personal data are accurate and up-to-date, informing the data controller without delay if the data controller becomes aware of the fact that the personal data he is processing are inaccurate or obsolete;

4. the obligations referred to in Article 32 of Regulation (EU) 2016/679.

d) The parties establish in Annex III the appropriate technical and organizational measures by which the controller is required to assist the controller in the application of this clause, as well as the scope and extent of the assistance requested.

## *Clause 9 - Notification of a personal data breach*

In the event of a personal data breach, the data controller cooperates with the data controller and assists him in fulfilling the obligations incumbent on the latter pursuant to articles 33 and 34 of regulation (EU) 2016/679 or articles 34 and 35 of Regulation (EU) 2018/1725, where applicable, taking into account the nature of the processing and the information available to the controller.

*9.1. Violation concerning data processed by the data controller*

In the event of a breach of personal data processed by the data controller, the data controller assists the data controller:

a) in notifying the personal data breach to the competent supervisory authority or authorities, without undue delay after the data controller becomes aware of it, if applicable (unless it is unlikely that the breach of personal data presents a risk for the rights and freedoms of individuals);

b) in obtaining the following information which, in accordance with Article 33, paragraph 3, of Regulation (EU) 2016/679, must be indicated in the notification of the data controller and include at least:

1. the nature of the personal data including, where possible, the categories and approximate number of data subjects concerned as well as the categories and approximate number of records of the personal data concerned;

2. the probable consequences of the breach of personal data;

3. the measures adopted or proposed to be adopted by the data controller to remedy the violation of personal data, if necessary also to mitigate any possible negative effects.

If, and to the extent, it is not possible to provide all information at the same time, the initial notification contains the information available at that time, and the other information is provided subsequently, as soon as available, without undue delay.

c) in fulfilling, in accordance with Article 34 of Regulation (EU) 2016/679, the obligation to communicate the violation of personal data to the interested party without undue delay, if the violation of personal data is likely to present a risk high for the rights and freedoms of individuals.

*9.2. Violation concerning data processed by the data controller*

In the event of a violation of personal data processed by the data controller, the latter notifies the data controller without undue delay after becoming aware of it. The notification contains at least:

d) a description of the nature of the infringement (including, where possible, categories and the approximate number of data subjects and data records in question);

e) the contact details of a contact point where further information on the breach of personal data can be obtained;

f) the probable consequences of the violation of personal data and the measures adopted or proposed to be adopted to remedy the violation, also to mitigate its possible negative effects.

If, and to the extent, it is not possible to provide all information at the same time, the initial notification contains the information available at that time, and the other information is provided subsequently, as soon as available, without undue delay.

The parties establish in Annex III all the other elements that the data controller is required to provide when assisting the data controller in fulfilling the obligations incumbent on the data controller pursuant to articles 33 and 34 of Regulation (EU) 2016 / 679.

## SECTION III - FINAL PROVISIONS

*Clause 10 - Non-compliance with the clauses and termination*

a) Without prejudice to the provisions of Regulation (EU) 2016/679, if the data controller violates his obligations under these clauses, the data controller may instruct the data controller to suspend the processing of personal data until the latter respects these clauses or the contract is terminated. The data controller promptly informs the data controller if, for any reason, he is unable to comply with these clauses.

b) The data controller has the right to terminate the contract regarding the processing of personal data in accordance with these clauses if:

1. the processing of personal data by the data controller has been suspended by the data controller in accordance with letter a) and compliance with these clauses is not restored within a reasonable time and in any case within one month of the suspension;

2. the data controller substantially or persistently violates these clauses or the obligations incumbent on him in accordance with Regulation (EU) 2016/679;

3. the controller fails to comply with a binding decision of a competent court or of the competent supervisory authority or authorities regarding its obligations in accordance with these clauses or with Regulation (EU) 2016/679.

c) The controller has the right to terminate the contract regarding the processing of personal data under these clauses if, after informing the controller that his instructions violate the applicable legal requirements in accordance with clause 7.1, letter b), the data controller insists on compliance with the instructions.

d) After the termination of the contract, the data controller, at the choice of the data controller, deletes all personal data processed on behalf of the data controller and certifies that he has done so, or returns all data to the data controller and delete existing copies, unless Union or Member State law requires the retention of personal data. As long as the data is not deleted or returned, the controller continues to ensure compliance with these clauses.

## ANNEX I - List of parts

| **Holder of the treatment**<br>(Customer) | |
|---|---|
| Name & Surname, Company<br>Address1<br>Address 2<br>VAT numebr Tap here to insert the text | |
| ☐ Responsable of the data | Contact |

Date Tap here to enter the date

Sign

| **Responsible for the treatment**<br>(DNAPhone) | |
|---|---|
| DNAPhone s.r.l.<br>Viale Mentana, 150 – 43121 Parma (IT)<br>C.F. e P.IVA. 02731440349 | |
| ☐ Responsible for data protection | Contact |

Date Tap here to enter the date.

Sign

# ANNEX II - DESCRIPTION OF THE TREATMENT

| | | |
|---|---|---|
| CATEGORIES OF INTERESTED PARTIES | Users registered with the Smart Analysis device. | |
| CATEGORIES OF PERSONAL DATA PROCESSED | Common data (name, surname, e-mail, phone number, login username, company name, country, location, usage and interaction data). | |
| SENSITIVE DATA PROCESSED AND GUARANTEES | N / A. | |
| NATURE OF THE PROCESSING | Automated processing. | |
| PURPOSE OF TREATMENT | Provision of backup & restore service. | |
| PURPOSE 1 | Periodic backup and restore. | |
| PURPOSE 2 | Test Function | |
| DURATION OF TREATMENT | The duration of the activated service follows. | |

The backup & restore service allows for the synchronization and recovery of analysis data, i.e. to have the data recorded in the archive (or historical) section of the dedicated APP. If you activate the service, you can see and act on the data that is synchronized on all the devices you have, after logging in to your account. In case of replacement or addition of an Android mobile device, you will have access to all synchronized information (after connecting to the internet). Once you have logged into your account, the APP will remain connected automatically until you log out: the synchronization and data recovery service will remain active without further actions by the user until the moment you log out of your account. Account means the personal access account created through the dedicated APPs: Smart Analysis, Smart Hub or at https://smart.dnaphone.it/, and which is necessary to use the Smart Analysis tool.

How the service works

The customer activates the paid service on one (or more) accounts linked to the Smart Analysis platform purchased, through the request to the address ordini@dnaphone.it, or by using the specific function indicated in the "ORDERS" section

The Backup & Restore mode is activated on the specific customer account, i.e. all the data saved in the APP archive are saved in a dedicated server and synchronized with all devices on which the same account is used.

The service is valid for one year and begins with the confirmation and payment of the same; it is automatically considered renewed for the following year.

The service can be deactivated upon written communication via email to ordini@dnaphone.it, at any time within the year of validity, and remains valid until the end of the year already activated.

If the customer who used the service decides to suspend it, and then resume it after a certain period of time, when the service is reactivated, the months / years in which the service was suspended must also be paid, with the consequent synchronization and recovery of data. relating to that period.

# ANNEX III - TECHNICAL AND ORGANIZATIONAL MEASURES, INCLUDING TECHNICAL AND ORGANIZATIONAL MEASURES TO ENSURE DATA SECURITY

The data synchronization and recovery service allow you to have the data recorded in the archive (or history) section of the APP.

If the service is activated, it is possible to see and act on the synchronized data on all the devices you have. In case of replacement / addition of a device, you will have access to all the synchronized information (after logging in to your account). Once logged into your account, the APP will remain automatically connected to the account until you log out.

The data synchronization and recovery service will remain active without further action on the part of the user until the moment he / she leaves his / her account (logout). By account we mean the DNAPhone account created in order to use the APP with the "Smart Analysis" analysis tool.

The data will be kept for the entire period in which the services associated with the Smart Analysis platform are used, to ensure the possibility of data recovery by the owner of the instrument. It is possible to expressly request the irreversible cancellation of data at any time, which will be carried out within 7 working days. The request must be made by means of a written notification to DNAPhone srl by the owner of the instrument or by whoever receives the proxy. The (personal) data are also deleted, while only those in anonymized form after 5 years of inactivity will be kept.

The data is also anonymized and stored separately from a second service for mainly statistical purposes and to improve the service.

The Data Sync and Retrieval Service uses two AWS servers.

A server (S1) anonymizes users by assigning UUID (Universally Unique IDentifier) codes.

Another server (S2) manages and stores the data collected and anonymized by S1. All collected data are stored by structuring relational databases.

The sending of information from the APP to the servers and from the servers to the APP are encapsulated in JSON format and are encrypted using the AES (Advanced Encryption Standard) 256 encryption protocol.

Encrypted objects are exchanged through communication with the Hypertext Transfer Protocol Secure (HTTPS) protocol. Data integrity is verified using the md5 cryptographic hash function.

The correct functionality of the service is guaranteed by periodic automated checks.

In case of prolonged malfunction beyond 24 hours, service interruption due to maintenance or unpredictable events, the user will be notified by e-mail and / or indication in the APP.

The data collected on AWS instances are located within the European Union (EU).

DNAPhone srl uses the AWS backup service, making a backup of the platform every 12 hours.

DNAPhone srl regulates and tracks the internal accesses intended for the management (maintenance, implementation, consultation) of the service through the management tools provided by AWS (https://aws.amazon.com/it/products/management-tools/).

An updated archive of people and access privileges is kept at the company headquarters.

## ANNEX IV - List of sub-processors

The data controller has authorized the use of the following sub-processors:

| | |
|---|---|
| Name & Surname, Company<br>Address 1<br>Address 2<br>VAT Number | |
| ☐ REsponsable for the data | Contact |
| Description of the data usage | |
| Tap to enter the text | |