JUNIO DE 2022

# DOCUMENTO DE PRIVACIDAD

**NORTON GREY, S.L**

Information clauses
Register of processing activities
Security measures
Rights Protocol
General Privacy Policy
Annexes

## GENERAL INFORMATION

This document has been designed for the processing of low-risk personal data, from which it follows that it may not be used for the processing of personal data that includes personal data relating to ethnic or racial origin, political, religious or philosophical ideology, trade union affiliation, genetic and biometric data, health data, and data on the sexual orientation of individuals, as well as any other data processing that entails a high risk to the rights and freedoms of individuals.

Article 5.1.f of the General Data Protection Regulation (hereinafter GDPR) determines the need to establish appropriate security safeguards against unauthorised or unlawful processing, against loss of personal data, accidental destruction or damage. This implies the establishment of technical and organisational measures aimed at ensuring the integrity and confidentiality of personal data and the possibility to demonstrate, as set out in Article 5(2), that these measures have been put into practice (*proactive accountability*).

Norton Grey, SL, undertakes to comply with everything detailed in this document and to keep it duly updated according to the activity of the company in relation to the use of personal data, thus having a proactive responsibility.

# INDEX

# 1.- INFORMATION SERVICE OF NORTON GREY,SL

Norton Grey, SL, is a commercial entity with tax identification number B-66854100 and tax domicile at (08001) Calle de Pelai nº 12, 3rd floor, Barcelona.
Its purpose is the development, integration and operation of V.A.S. (Value Added Services) services for cellular telephony. Performing an intermediary service in the communication of SMS messages between the provider companies and their customers, acting as a mere messaging intermediary without entering into the content of the SMS messages sent, as well as without being able to know and identify any of the owners of the telephone lines to which the SMS messages are sent, since Norton Grey's customers send anonymised data.

Anonymous information is a set of data that does not relate to an identified or identifiable natural person (Recital 26 of the GDPR), while pseudonymised information is a set of data that cannot be attributed to a data subject without the use of additional information, requires that such additional information is separately identified and, in addition, is subject to technical and organisational measures designed to ensure that personal data are not attributed to an identified or identifiable natural person (Article 4(5)).

The processing that generates the anonymised data is indeed a processing of personal data, which can be considered compatible with the original purpose of the processing of personal data from which the data originate (Opinion 05/2014 on anonymisation techniques WP246, paragraph 2.2.1.)

In other words, the data will be considered anonymised to the extent that there is no reasonable probability that any person can identify the natural person in the data set (Recital 26), since NORTON GREY,SL without the additional information provided by its customers cannot identify any natural person, with the data it manages for the performance of the service to be provided, which is no more than that of intermediation in telecommunications.

# 2.- INFORMATIVE CLAUSES

## 2.1.- PROCESSING OF POTENTIAL CUSTOMER DATA

**Information clause**:

**The following text should be included in all forms you use to collect personal data from your potential customers, whether you collect it on paper or via a web form.**

*"At NORTON GREY we process the information you provide in order to provide you with the requested service or to send you the requested information. The data provided will be kept as long as you do not request us to cease the activity. The data will not be passed on to third parties except in cases where there is a legal obligation.*

*You have the right to obtain information about whether we at NORTON GREY are processing your personal data, so you can exercise your ARSOPOL rights to the e-mail address* data@nortongrey.com *attaching a copy of your ID card or equivalent document. Likewise, and especially if you consider that you have not obtained full satisfaction in the exercise of your rights, you may file a complaint with the national supervisory authority by contacting the AEPD, C/ Jorge Juan, nº6, (28001)Madrid*".

## 2.2.- PROCESSING OF SUPPLIER DATA

**Information clause**:

**The following text should be included in all forms you use to collect personal data from suppliers or in the invoices you issue.**

*"In compliance with the provisions of the RGPD, relating to the protection of personal data and the free movement of the same, we inform you that the data you provide will be incorporated and processed in the files owned by NORTON GREY, in order to be able to provide you with our services, as well as to keep you informed on matters relating to the activity of the company. NORTON GREY undertakes to treat the personal data provided as confidential and not to communicate or transfer this information to third parties. In accordance with the aforementioned Law, you are entitled to exercise ARSOPOL's rights free of charge by sending an e-mail to data@nortongrey.com".*

## 2.3.-TREATMENT FOR STAFF OR COLLABORATOR:

In compliance with the General Data Protection 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 and on the free movement of such data, and the Organic Law 3/2018 of 5 December on the Protection of Personal Data and the guarantee of digital rights and implementing regulations, by signing this ANNEX to the employment contract, the undersigned employee gives his/her express consent to the processing of personal data by the employer solely for the purposes set out in the contractual relationship.

To this effect, you are hereby informed that if you wish to exercise your ARSOPOL rights to the processing of your data, this should be done by sending an e-mail to the following address: data@nortongrey.com

In addition, the employee expressly authorizes the employer company to transfer their data to an authorized third party for the same purposes, specifically to **LA GESTORIA DE SANT FELIU DE LLOBREGAT, SL**, who will be responsible for the processing of data only for the preparation of payroll, social security and income tax, in full compliance with data protection regulations, this end is expressly authorized as an annex to the contract of employment of workers, is attached to this model document as Annex I.

### 2.4.-E-MAIL CLAUSE:

*"This e-mail contains private and strictly confidential information. If you are not the addressee of this message, you are not authorised to read, retain or disseminate it. E-mail does not ensure the confidentiality or proper receipt of messages, so if you do not agree to its use, please let us know. In accordance with the RGPD, we remind you that your data are under the responsibility of NORTON GREY, SL, and that they will not be passed on to third parties. You may exercise your ARSOPOL rights by sending an e-mail to* data@nortongrey.com.

## 3.- REGISTER OF PROCESSING ACTIVITIES

**The controller must review the data recorded in the sections of the Processing Activity Logs generated and verify that they correspond to the exact circumstances of the data collected, the communications made and other conditions of each of the processing operations.**

Treatment: **Clients**

| | | |
|---|---|---|
| a) | Controller | Identity: NORTON GREY,SL - NIF: B-66854100<br>Postal address:<br>(08001) Calle de Pelai nº 12, 3rd floor, Barcelona. |
| b) | Purpose of processing | Relationship management with potential customers |
| c) | Categories of stakeholders | Potential customers: Persons with whom a business relationship is sought as customers. |
| d) | Data categories | Those necessary for the commercial promotion of the company<br>Identification: name and surname and postal address, telephone numbers, e-mail address, etc. |
| e) | Categories of addressees | It is not envisaged |
| f) | International transfers | No international transfers are foreseen, although for the execution of the contract and taking into account that the company is based in Kenya, there is data consultation, but no data flow, and the data is always hosted in Spain. |
| (g) | Time limit for deletion | One year since first contact |
| h) | Security measures | Those reflected in the SAFETY MEASURES section. |

Processing: **Suppliers**

| | | |
|---|---|---|
| a) | Controller | Identity: NORTON GREY,SL - NIF: B-66854100<br>Postal address: |

| | | |
|---|---|---|
| | | (08001) Calle de Pelai nº 12, 3rd floor, Barcelona. |
| b) | Purpose of processing | Supplier relationship management |
| c) | Categories of stakeholders | Suppliers: Persons with whom a business relationship is maintained as suppliers of products and/or services. |
| d) | Data categories | Those necessary for the maintenance of the employment relationship<br>Identification: name, tax identification number, postal address, telephone numbers, e-mail address<br>Bank details: for direct debit of payments |
| e) | Categories of addressees | State Agency for Tax Administration<br>Banks and financial institutions<br>Partners |
| f) | International transfers | No international transfers are foreseen, although for the execution of the contract and taking into account that the company is based in Kenya, there is data consultation, but no data flow. And the data is always hosted in Spain. |
| (g) | Time limit for deletion | Those provided for by tax legislation regarding the statute of limitations for liabilities |
| h) | Security measures | Those reflected in the SAFETY MEASURES section. |

Treatment: **Staff/Collaborators**

| | | |
|---|---|---|
| a) | Controller | Identity: NORTON GREY,SL - NIF: B-66854100<br>Postal address:<br>(08001) Calle de Pelai nº 12, 3rd floor, Barcelona. |
| b) | Purpose of processing | Relationship management with external partners/professionals |
| c) | Categories of stakeholders | Partners: Persons with whom we seek to maintain a business relationship as professional partners. |
| d) | Data categories | Those necessary for the development of joint projects.<br>Identification: name and surname and postal address, telephone numbers, e-mail, professional membership details. |
| e) | Categories of addressees | It is not envisaged |
| f) | International transfers | No international transfers are foreseen |
| (g) | Time limit for deletion | One year since first contact |
| h) | Security measures | Those reflected in the SAFETY MEASURES section. |

Title: **Corporate website**

| | | |
|---|---|---|
| a) | Controller | Identity: NORTON GREY,SL - NIF: B-66854100<br>Postal address:<br>(08001) Calle de Pelai nº 12, 3rd floor, Barcelona. |
| b) | Purpose of processing | Relationship management with external partners/professionals |
| c) | Categories of stakeholders | Partners: Persons with whom we seek to maintain a business relationship as professional partners. |
| d) | Data categories | Those necessary for the development of joint projects.<br>Identification: name and surname and postal address, telephone numbers, e-mail, professional membership details. |
| e) | Categories of addressees | It is not envisaged |
| f) | International transfers | No international transfers are foreseen |
| (g) | Time limit for deletion | One year since first contact |
| h) | Security measures | Those reflected in the SAFETY MEASURES section. |

# 4.- SECURITY MEASURES

The minimum security measures you should consider are as follows:

## 4.1 ORGANISATIONAL MEASURES

INFORMATION WHICH SHOULD BE KNOWN TO ALL STAFF WITH ACCESS TO PERSONAL DATA:

All staff with access to personal data shall be made aware of their obligations in relation to the processing of personal data and shall be informed of those obligations. The minimum information that shall be known to all staff shall be as follows:

- **DUTY OF CONFIDENTIALITY AND SECRECY**
    - Access to personal data by unauthorised persons shall be prevented. To this end, leaving personal data exposed to third parties (unattended electronic screens, paper documents in publicly accessible areas, media containing personal data, etc.) shall be avoided. This includes screens used for the display of images from the video surveillance system. When absent from the workstation, the screen shall be locked or the session shall be closed.
    - Paper documents and electronic media shall be stored in a secure place (lockers or restricted access rooms) 24 hours a day.
    - Documents or electronic media (CDs, pen drives, hard disks, etc.) containing personal data shall not be discarded without ensuring their effective destruction.
    - No personal data or other information of a personal nature shall be disclosed to third parties, with particular attention being paid to not disclosing protected personal data during telephone enquiries, e-mails, etc.
    - The duty of secrecy and confidentiality persists even when the employee's employment relationship with the company ends.

- **PERSONAL DATA SECURITY BREACHES**
    - When security breaches of personal data occur, such as, for example, theft or improper access to personal data, the Spanish Data Protection Agency shall be notified within 72 hours of such security breaches, including all the information necessary to clarify the facts that have given rise to the improper access to the personal data. The notification shall be made by electronic means through the electronic headquarters of the Spanish Data Protection Agency at the address https://sedeagpd.gob.es/sede-electronica-web/.

## 4.2 TECHNICAL MEASURES

**IDENTIFICATION**

- Where the same computer or device is used for personal data processing and personal use purposes, it is recommended to have several different profiles or users for each purpose. Professional and personal use of the computer should be kept separate.
- It is recommended to have profiles with administration rights for installation and configuration of the system and users without privileges or administration rights for access to personal data. This measure will prevent access privileges from being obtained or the operating system from being modified in the event of a cybersecurity attack.
- Passwords shall be ensured for access to personal data stored in electronic systems. The password shall be at least 8 characters, a mixture of numbers and letters.
- Where personal data are accessed by different persons, for each person with access to the personal data, a specific user name and password (unambiguous identification) shall be available for each person with access to the personal data.
- The confidentiality of passwords must be guaranteed, preventing them from being exposed to third parties.

**DUTY TO SAFEGUARD**

The following are the minimum technical measures to ensure the safeguarding of personal data:

- **UPDATING OF COMPUTERS AND DEVICES**: Devices and computers used for the storage and processing of personal data shall be kept up to date to the extent possible.
- **MALWARE**: On computers and devices where automated processing of personal data is carried out, an anti-virus system shall be in place to ensure as far as possible the theft and destruction of personal information and data. The anti-virus system shall be updated on a regular basis, a regular update system for malware is available.

- **FIREWALL**: In order to avoid undue remote access to personal data, it shall be ensured that a firewall is activated and correctly configured on those computers and devices where personal data is stored and/or

processed. There is currently an adequate firewall in force for the company's two laptops.

- **DATA ENCRYPTION**: When the extraction of personal data outside the premises where the processing is carried out, whether by physical or electronic means, an encryption method should be considered to ensure the confidentiality of personal data in case of improper access to the information.
- **SECURITY COPY**: A backup copy shall be made periodically on a second medium other than the one used for daily work. The copy will be stored in a safe place, different from the one where the computer with the original files is located, in order to allow the recovery of personal data in case of loss of information, currently a copy is made in the cloud of the Microsoft drive, which is a correct and sufficient measure.

Security measures will be reviewed on a regular basis, either by automatic mechanisms (software or computer programmes) or manually. Consider that any computer security incident that has happened to anyone you know can happen to you, and guard against it.

## Device inventory and management software

**A.- Computer equipment:**

3 desktops-Lenovo
i56400
-HP ProDesk G5 9500
-Asus PcCom Mini Asus Intel Core i3-1115G4/8GB/240GB SSD
-Microsoft Surface Laptop, Microsoft Windows 11 home-Apple Macbook Air M1, MacOS Monterey 12.4
-Macbook Pro 13
-Ipad Pro: ML0F2FD/A
-1 HP Officejet 4630 Printer

Company telephones:
Apple Iphone 13 ProSamsung
Galaxy Tab S7 FE, Android 12, One UI 4.1Samsung
Galaxy S21 S21 Ultra 5G, Android 12, One U1 4.1Samsung
Galaxy S9+, Android 10, One UI 2.5

**B.- Management software:**
Desktop: Windows 10
Mac: MacOs Catalina 10.15.7

**C.- Storage and security copies:** Backup to a network hard disk, located at the company's registered office. In addition, an extra back-up copy is made in which the

telecommunications solution located at Passeig Maragall 207, mezzanine 3ª in Barcelona is duplicated, which is equipped with security cameras and restricted access, only authorised by the company manager.

As a legal recommendation and according to the telecommunications law, specifically article 5, the maximum time for storing transaction data is 2 years.
https://www.boe.es/buscar/act.php?id=BOE-A-2007-18243

**Hard disk:**
Brand: Seagate
Model:STGX5000400
Capacity: 5TB

**D.- Data sharing applications**: Google Drive
**E.- Protection System:** McAfee Antivirus

Data processors of NORTON GREY,SL with whom there is a data processor contract in force.

a.- Management/Company consultancy:

LA GESTORIA DE SANT FELIU DE LLOBREGAT, S.L.
Ctra. Laureà Miró, 107
Tel. 936669276
Email: asesoria@gazquezycia.es

# 5.- ARSOPOL PROTOCOL

## 5.1.- INTRODUCTION

The Data Controller has established the following internal protocol or procedure for the purpose of regularising the exercise of the rights known as ARSO-POL; access, rectification, deletion, opposition, portability, forgetfulness and limitation of data subjects.
The purpose of this document is to provide the people in the company responsible for processing them with a guide that establishes the guidelines to be followed for the correct treatment of the same.
They are very personal rights and this means that they can only be exercised by the person concerned, with 2 exceptions:

- When the affected person is in a situation of incapacity or minority that prevents him/her from exercising these rights in person, they may be exercised by his/her legal representative, in which case it will be necessary that he/she accredits such condition.

- The rights may also be exercised through a voluntary representative, expressly designated for the exercise of the right. In this case, the identity of the represented party must be clearly accredited, by providing a copy of their National Identity Document or equivalent document, and the representation conferred by them.

In any case, ARSO-POL rights are independent rights, so that the exercise of any one of them cannot be understood as a prerequisite for the exercise of another.

The data subject must be provided with a simple and free means of exercising these rights, and under no circumstances may this entail additional income for the data controller before whom they are exercised. Even if the data subject has not used the procedure established by the data controller for the exercise of ARSOPOL rights, a response must be given in the same manner in due time and form, provided that the receipt of the same can be accredited.

### 5.2.- REQUIREMENTS

Except in the case in which the data controller has a customer service department or for the exercise of claims related to the service provided, the exercise of the right must be carried out by means of a communication addressed to the Data Controller.

In order to exercise this right, the data subject must send a written request, in all cases providing the following information:

- Name and surname of the person concerned.
- National ID card or legally valid identification document.
- Postal address for notification purposes.
- The request in which the application is made.
- Documents accrediting the request made.
- Date and signature of applicant

Under no circumstances should exercises of ARSO-POL rights via telephone be accepted.

In any case, the data controller must reply to the request addressed to him/her in any case, regardless of whether or not the data subject's personal data are included in his/her files. In the event that the request does not meet the requirements specified above, the data controller must request the correction of the same.

The data controller shall adopt the appropriate measures to ensure that the persons in his organisation who have access to personal data can inform of the procedure to be followed by the data subject to exercise his rights.

### 5.3.- MANAGEMENT AND DOCUMENTATION

Legislation regulates the deadlines for processing and replying to ARSO-POL rights, which have a very short response period that must be complied with, both positively and negatively, as appropriate. Any exercise of rights must always be recorded immediately by informing the person responsible for its management.

### 5.4.- EXPLANATORY DETAIL ARSOPOL RIGHTS

| | | |
|---|---|---|
| **ACCESS** | The right of access is the right of the data subject to obtain information on whether his or her own personal data are being processed, the purpose of the processing which, if any, is being carried out, as well as the information available on the origin of | Maximum time limit of 1 month to reply from receipt of the request |

| | | |
|---|---|---|
| | such data and the communications made or envisaged of the same. | |
| **RECTIFICATION** | The right of rectification is the right of the data subject to have inaccurate or incomplete data amended. | Maximum of 10 days to reply from receipt of the request. |
| **SUPPRESSION** | The right of the holder of personal data to obtain without undue delay the erasure of personal data concerning him/her, provided that a number of circumstances are met. | Maximum of 10 days to reply from receipt of the request. |
| **OPPOSITION** | The right of objection is the right of the data subject not to have his or her personal data processed or to cease processing in the following cases:<br>1. When your consent to the processing is not necessary, as a consequence of the concurrence of a legitimate and well-founded reason, referring to your specific personal situation, which justifies it, provided that a Law does not provide otherwise.<br>2. In the case of files whose purpose is to carry out advertising and commercial prospecting activities, regardless of the company responsible for their creation.<br>3. Where the purpose of the processing is the adoption of a decision relating to the data subject and based solely on automated processing of his or her personal data. | Maximum of 10 days to reply from receipt of the request. |
| **PORTABILITY** | This right is an advanced form of the right of access, whereby the copy provided to the data subject must be in a structured, commonly used and machine-readable format. It implies that the data subject's personal data are transmitted directly from one controller to another, without the need for the data subject to go through the user (where technically possible). And it is based on certain assumptions of legal legitimacy. | Maximum of 10 days to reply from receipt of the request. |
| **FORGET** | This right is not considered an autonomous or distinct right from the ARCO rights, but the consequence of the application of the right to erasure of personal data. It establishes the | Maximum of 10 days to reply from receipt of the request. |

| | | |
|---|---|---|
| | deletion of personal data when any of the cases envisaged occur, for example, the unlawful processing of the data, or the disappearance of the purpose of the processing. According to the AEPD, it is a manifestation of the rights of cancellation or opposition in the online environment. | |
| **LIMITATION** | This right entails the marking of personal data stored for the purpose of limiting their processing in the future, when some of the conditions set out in the precept regulating it are met (art. 18 RGPD). | Maximum of 10 days to reply from receipt of the request. |

**PROCEDURE**: When exercising any ARSOPOL right, the data subject may opt for one or several of the following file consultation systems, provided that the configuration or material implementation of the file allows it, and it will be sent in digital format and by e-mail.

The following steps should be taken in this regard:

⇒ Notify the person responsible for the exercise of rights of the receipt of the request.

⇒ Check that the application is correct. If this is not the case, a registered letter rejecting the claim must be sent, stating the reason.

For the duty to be considered correct, it must be satisfied that:

- The person exercising the right is either the affected person himself or his legal representative. In the case of the second option, proof of representation must be provided.
- That this right has not been exercised in the last 12 months, unless a legitimate interest is demonstrated, in which case it may be exercised earlier.
- Access may be refused where there is a directly applicable law or rule of Community law or where these prevent the Controller from disclosing to data subjects the processing of the data to which the access relates.

⇒ Proceed to obtain the personal data of the data subject existing in the files.

⇒ Send the data to the data subject within the established deadline.

In addition to the right of access, it is clear that the data subject may exercise the rights of deletion, rectification and objection, for which reason it will be necessary to indicate the data to be deleted or rectified, providing new data and documentary proof of the change, or to indicate the processes in which he/she wishes to be excluded.

## 6.- General Privacy Policy of NORTON GREY,SL

In compliance with the provisions of current legislation on personal data protection, NORTON GREY,SL, with address at (08001) Calle de Pelai nº 12, 3rd floor, Barcelona, informs on how the data of the people who contact our Organisation are collected, used and kept:

NORTON GREY,SL, CIF: B-66854100 and Address: (08001) Calle de Pelai nº 12, piso 3ªA, Barcelona.
and contact e-mail: data@nortongrey.com

**PURPOSES OF THE PROCESSING** - The processing of the data is carried out for the purpose of being able to provide the services for which we have been contracted or for the execution of any request, consultation or management.

**DURATION OF THE TREATMENT** - The data will be kept for as long as the service provision order is in force. Once the relationship has ended, the data may be kept for the maximum time required by the applicable legislation and up to a maximum of ten (10) years in accordance with money laundering legislation.

**LEGITIMACY FOR THE PROCESSING OF DATA** - The legal basis for the processing of your data for the purposes set out in this document lies in the execution of the corresponding Services.

**COMMUNICATION OF DATA -** The data, where appropriate, communicated to the following entities:

- Competent public authorities, Treasury, in specific relation only to the provision of the relevant service.
- To the financial institutions through which the management of collections and payments is articulated.
- Business consultancy: La Gestoria de Sant Feliu de Llobregat, SL, Ctra. Laureà Miró,107, Mail: asesoria@gazquezycia.es

**RIGHTS**: All interested parties who provide their data have the following rights:
Any person has the right to obtain confirmation as to whether we are processing their personal data, having the right to ACCESS their personal data, as well as to request the RECTIFICATION of inaccurate data or, where appropriate, to request its DELETION when the data is no longer necessary for the purposes for which it was collected.

Under the conditions of the General Data Protection Regulations, any data subject may request the LIMITATION of the processing of their data or their PORTABILITY, in which case we will only keep their data for the exercise or defence of claims.

In certain circumstances and for reasons relating to your particular situation, you may object to the processing of your data. If you have given consent for a specific purpose, you have the right to withdraw your consent at any time, without affecting the unlawfulness of the processing based on the consent prior to its withdrawal. In these cases we will stop processing the data for the specific purpose, except for legitimate reasons or for the exercise or defence of possible claims.

The aforementioned rights may be exercised through the means of contact listed in the "Data Controller" section above.
In the event of any violation of your rights, especially when you have not obtained satisfaction in the exercise of your rights, you can file a complaint with the Spanish Data Protection Agency (data accessible at www.agpd.es) or with any competent supervisory authority.

**THIRD PARTY DATA** - With regard to the third party data provided to us, you assume the responsibility of informing them in advance of all the provisions of the RGPD and the LOPDGDD in the conditions established for this purpose.

## ANNEX I.- Labour Contract Clause

**ANNEX TO THE DATE CONTRACT_____**
**DATA PROTECTION CLAUSE**

In compliance with 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, "GDPR"), Organic Law 3/2018 of 5 December, on the Protection of Personal Data and guarantee of digital rights (hereinafter, "LOPDGDD") and implementing regulations, by signing this ANNEX to the employment contract, the undersigned employee expressly consents to the processing of personal data by the employer solely for the purposes established in the contractual relationship. To this effect, you are hereby informed that, if you wish to exercise your rights of Access, Rectification, Deletion, Opposition, Limitation and Portability to the processing of your data, this must be done by electronic communication to _____ of the company, attaching a copy of your ID card.

Furthermore, the employee expressly authorises the employer company to transfer his or her data to an authorised third party for the same purposes, namely to the company _____, which will be responsible for processing the data solely for the purposes of payroll, social security and personal income tax, in full compliance with data protection regulations.

SIGNATURE

## ANNEX II - Model Confidentiality for Workers

**Confidentiality Document Workers**

It is hereby declared that the worker ..... with D.N.I. ..... is the user of the data of the person in charge ..... domiciled and with N.I.F. ....., and,

**RECOGNISES**

That he/she has been informed of the security measures adopted by the data controller for the correct protection of the data subjects' data and that he/she is aware of the following obligations, knowing that failure to comply with them may give rise to administrative liability.

a. Duty of confidentiality and secrecy

    i. Access to personal data by unauthorised persons shall be prevented by avoiding: leaving personal data exposed to third parties (unattended electronic screens, paper

documents in public access areas, media with personal data, etc.). When absent from the workstation, the screen shall be locked or the session shall be closed.

ii. Paper documents and electronic media shall be stored in a secure place (lockers or restricted access rooms) 24 hours a day.

iii. Documents or electronic media (CDs, pen-drives, hard disks, etc.) containing personal data shall not be discarded without guaranteeing their destruction.

iv. Personal data or any personal information shall not be disclosed to third parties. Particular care shall be taken not to disclose protected personal data during telephone enquiries, e-mails, etc.

v. The duty of secrecy and confidentiality persists even when the employee's employment relationship with the company ends.

b. Rights of data subjects. The holders of personal data may exercise their rights of access, rectification, deletion and opposition upon presentation of their ID card. For this purpose, the employee to whom the data subject addresses himself/herself will provide him/her with an e-mail address of the data controller for him/her to contact him/her.

c. In the event of security breaches of personal data, such as theft or improper access to personal data, the controller shall be notified no later than 72 hours after such security breaches, including all information necessary to establish the facts that led to the improper access to the personal data.

And so,

**ACCEPT**

DATE :..... SIGNED:
.....

## ANNEX III.- Model Data Processor Contract

**PERSONAL DATA PROCESSING AGREEMENT BETWEEN "NORTON GREY, SL" and "_____".**

*"In accordance with Chapter IV of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of personal data of natural persons with regard to the processing of personal data and on the free movement of such data."*

**MEETING**

On the one hand, _____, of legal age, of nationality _____ with business address for these purposes at (CP) City, Address, and holder of D.N.I.N/N.I.F number _____.

And, of the other part, _____, of legal age, of nationality _____, with professional address for these purposes at (CP) City, Address and holder of D.N.I/N.I.F number _____.

**INTERVENE**

**I.-** _____ in the name and on behalf of _____ company of Spanish nationality, with registered office at _____-. Incorporated for an indefinite period of time by virtue of a deed authorised by the Notary _____, on ____, under protocol number _____ and registered _____- and with C.I.F. number _____.

The person appearing in the present contract exercises this representation in his capacity as _____, a position for which he was appointed in the same deed and which has not been revoked at the date of signature of the present contract. This party is hereinafter referred to as "THE RESPONDENT".

**II.-** _____, in the name and on behalf of the trading company _____, a company of Spanish nationality, with registered office at _____, constituted for an indefinite period of time by virtue of a deed authorised by the Notary Public d_____, dated under number _____ of his protocol and registered in the Mercantile Register of _____, with tax identification number _____:

The undersigned exercises such representation in his capacity as _____, a position for which he was appointed in the same deed and which has not been revoked at the date of signature of this contract. This party will hereinafter be referred to as "THE AGENT".

Both parties mutually and reciprocally recognise each other's legal capacity and the necessary and sufficient representation to contract and bind themselves, in particular to sign this contract, for which they hereby **state** as background information:

I.- That both parties are bound by a relationship of provision of services consisting of:

a.- _____
b.- _____
c.- _____
d.- _____

**II.-** That in order to provide said services it is necessary for the CARRIER to have access to the personal data for the processing of which it is RESPONSIBLE.

That, on the basis of the foregoing, and in compliance with Article 28 of the European Union Regulation 2016/679, of 27 April, on the Protection of Personal Data, both parties of their free and spontaneous will agree to regulate this access and processing of personal data in accordance with the following **CLAUSES**:

**FIRST**: Access by the RESPONSIBLE PARTY to the personal data held by the RESPONSIBLE PARTY will not be considered communication of personal data.

**SECOND**: The RESPONSIBLE PARTY makes available to the CARRIER all the data necessary for the correct provision of its services.

**THIRD**: The RESPONSIBLE PARTY hereby states that the data made available to the CHARGEEES are duly protected, in compliance with the security measures provided for in articles 32 to 36 of the RGPD, and which are determined by regulation. That is, all those technical and organisational measures necessary to guarantee the security of personal data and prevent its alteration, loss, unauthorised processing or access, taking into account the state of technology, the nature of the data stored and the risks to which they are exposed, whether from human action or from the physical or natural environment. In the event that the RESPONSIBLE PARTY cannot guarantee compliance with such measures, the CONTROLLER will assist it in complying with its obligation to respond to requests aimed at exercising the rights of data subjects established in Chapter III of the aforementioned Regulation.

**FOURTH:** Access on behalf of the CHARGEEER to the personal data held by the RESPONSIBLE will be reused solely and exclusively for the stipulated purpose, so that the CHARGEEER can provide the RESPONSIBLE PARTY with the agreed services.

**FIFTH:** The CARRIER will process the personal data only in accordance with the instructions of the CONTROLLER of the processing, including with regard to transfers of personal data to a third country, unless it is obliged to do so by virtue of Union or Member State law that applies to the CARRIER; in such a case, the CARRIER will inform the CONTROLLER of this legal requirement prior to processing, unless such law prohibits it for important reasons of public interest.

**SIXTH -** The PROCESSOR undertakes to maintain professional secrecy with regard to the personal data access to which is regulated by this contract, and all its personnel undertake to:

a) Use the personal data undergoing processing, or those collected for their inclusion, only for the purpose of this order. Under no circumstances may it use the data for its own purposes.
b) Process the data in accordance with the instructions of the controller. If the processor considers that any of the instructions violate the GDPR, the GDPR or any other Union or Member State data protection provisions, the processor shall immediately inform the controller.
c) Keep, in writing, a record of all categories of processing activities carried out on behalf of the controller, where there are more than 250 employees, or the processing is likely to result in a risk to the rights and freedoms of data subjects and is not occasional, or involves special categories of data or personal data relating to criminal convictions or offences.

   Content of the Register of Processing Activities:
   1. The name and contact details of the processor(s) and of each controller on whose behalf the processor is acting and, where applicable, of the representative of the controller or processor and of the data protection officer.
   2. The categories of processing operations carried out on behalf of each controller.
   3. Where applicable, transfers of personal data to a third country or international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1) of the GDPR, documentation of appropriate safeguards.

4. A general description of the technical and organisational security measures relating to:

    a) Anonymisation and encryption of personal data.
    b) The ability to ensure the continued confidentiality, integrity, availability and resilience of processing systems and services.
    c) The ability to restore availability and access to personal data quickly, in the event of a physical or technical incident.
    d) The process of regular verification, evaluation and assessment of the effectiveness of technical and organisational measures to ensure the security of processing.

d) Not to communicate the data to third parties, except with the express authorisation of the data controller, in the legally admissible cases.

The processor may disclose data to other processors of the same controller, in accordance with the instructions of the controller. In this case, the controller shall identify, in advance and in writing, the entity to which the data are to be communicated, the data to be communicated and the security measures to be applied in order to proceed with the communication.

If the processor has to transfer personal data to a third country or to an international organisation under Union or Member State law applicable to it, it shall inform the controller of that legal requirement in advance, unless such law prohibits it for important reasons of public interest.

e) Subcontracting

Not to subcontract any of the services forming part of the object of this contract that involve the processing of personal data, except for auxiliary services necessary for the normal operation of the services of the person in charge.

If it is necessary to subcontract any processing, this must be communicated in writing to the data controller at least one (1) month in advance, indicating the processing to be subcontracted and clearly and unequivocally identifying the subcontracting company and its contact details. Subcontracting may not be carried out without the prior authorisation of the data controller.

The subcontractor, who shall also have the status of processor, is also obliged to comply with the obligations set out in this document for the processor and the instructions issued by the controller.

According to Article 28(4) of the GDPR, it is for the initial processor to regulate the new relationship, whether by contract or other legal act established under Union or Member State law, so that the new processor is subject to the same obligations, and to the same formal requirements, as regards the proper processing of personal data and the guarantee of the rights of the data subjects. In particular, the obligation to provide sufficient guarantees for the implementation of appropriate technical and

organisational measures so that the processing complies with the provisions of the GDPR and the LOPDGDD.

In the event of non-compliance by the sub-processor, the initial processor shall remain fully liable to the controller for the fulfilment of the obligations.

f) Maintain the duty of secrecy with regard to personal data to which it has access by virtue of this assignment, even after the end of the assignment.
g) Ensure that persons authorised to process personal data undertake, expressly and in writing, to respect confidentiality and to comply with the corresponding security measures, of which they must be duly informed.
h) Keep at the disposal of the person responsible the documentation accrediting compliance with the obligation established in the previous section.
i) Ensure the necessary training in personal data protection for persons authorised to process personal data.
j) Assist the controller in responding to the exercise of the rights of:
    1. Access, rectification, erasure and opposition
    2. Treatment limitation
    3. Data portability

    When the data subjects exercise their rights of access, rectification, erasure, objection, restriction of processing, data portability, the data processor must communicate this by e-mail to the address _____.
    The communication must be made immediately and in no case later than the working day following receipt of the request, together, where appropriate, with any other information that may be relevant to the resolution of the request.
k) Right to information

If the Data Processor is to collect personal data, it must inform the data subject on behalf of the Data Controller at the time of collection, following the indications and providing the information indicated by the Data Controller.

l) Notification of data security breaches

The processor shall notify the controller, without undue delay, and in any event no later than 48 hours, and via the email address indicated by the controller, of any breach of security of the personal data under its responsibility of which it becomes aware, together with all relevant information for the documentation and communication of the incident. Notification shall not be necessary when such breach of security is unlikely to constitute a risk to the rights and freedoms of natural persons.

If available, at least the following information shall be provided:

a) Description of the nature of the personal data breach, including, where possible, the categories and approximate number of data subjects affected, and the categories and approximate number of personal data records affected.
b) The name and contact details of the data protection officer or other point of contact where further information can be obtained.
c) Description of the possible consequences of the personal data security breach.

d) Description of the measures taken or proposed to be taken to remedy the personal data breach, including, where appropriate, measures taken to mitigate possible negative effects. If and to the extent that it is not possible to provide the information simultaneously, the information shall be provided in a phased manner without undue delay.
e) Support the controller in carrying out data protection impact assessments, where appropriate.
f) Support the controller in carrying out prior consultations with the supervisory authority, where appropriate.
g) Make available to the controller all information necessary to demonstrate compliance with his or her obligations, as well as for audits or inspections to be carried out by the controller or another auditor authorised by the controller.
h) Implement the security measures indicated by the Controller following an impact assessment or, in any case, implement mechanisms in the case of automated processing to:

    a) Ensure the continued confidentiality, integrity, availability and resilience of processing systems and services.

    (b) restore availability and access to personal data in a timely manner in the event of a physical or technical incident.

    (c) pseudonymise and encrypt personal data, if necessary.

    In the processing of paper documents and when new technologies are used:

    a) Regularly verify, evaluate and assess the effectiveness of the technical and organisational measures implemented to ensure the security of the processing.

m) Designate a data protection officer and communicate his or her identity and contact details to the data controller, if applicable.
n) Destination of data

    Return to the data controller the personal data and, if applicable, the media on which they are stored, once the service has been provided.
    The return must entail the complete erasure of the data existing on the computer equipment used by the data processor.
    However, the processor may keep a copy, with the data duly blocked, for as long as liability may arise from the performance of the service.

**SEVENTH**: The CONTROLLER shall ensure that the persons authorised to process the personal data have undertaken to respect confidentiality or are subject to a statutory confidentiality obligation and shall make available to the RESPONSIBLE PARTY all the necessary information on the persons authorised to process the personal data. It shall also report any breach of data security to the Data Protection Authority.

And it shall not transfer the management of the data to another data processor without the express authorisation of the data controller, who must inform of any change.
**EIGHTH:** The RESPONSIBLE PARTY is exonerated from any liability that may arise due to non-compliance by the PRINCIPAL with the stipulations of this contract, and specifically:

a.- In the event that the PROCESSOR uses or intends to use the personal data for any purpose other than that agreed and accepted by both parties;

b.- For the breach by said CARRIER of the duty incumbent upon him/her to keep them secret, and not to communicate them to third parties.

c.- For using the data in breach, in any way, of the stipulations of this contract.

**NINTH**: The CONTROLLER of the processing undertakes to:

a) To provide the person in charge with all the data necessary for the performance of the services.
b) Carry out an assessment of the impact on the protection of personal data of the processing operations to be carried out by the processor.
c) Conduct prior consultations as appropriate
d) Ensure prior to and throughout the processing that the processor complies with the RGPD and the LOPDGDD.
e) Overseeing treatment, including carrying out inspections and audits.

**TENTH**. - For any divergence that may arise from the interpretation, application and execution of this contract, the Courts and Tribunals of Barcelona shall have jurisdiction, and the parties waive any other jurisdiction that may correspond to them.

**IN WITNESS WHEREOF**, for the appropriate purposes, both parties, pledging themselves to the most faithful compliance with these agreements, have signed and, in witness whereof, have signed the present contract in duplicate and to a single effect at _____, at ____ of ____ of _____.

| | |
|---|---|
| THE RESPONSIBLE | THE PERSON IN CHARGE |
| "NORTON GREY,SL" | "_____" |
| P.p | P.p |
| S.D. | S.D. |