

# GENERAL CONDITIONS FOR THE BITNOVO REFERRAL PROGRAMME

## INDEX

<b><u>1.- LEGAL INFORMATION.</u></b>	<b>3</b>
<b><u>2.- OBJECT.</u></b>	<b>3</b>
<b><u>3.- CHARACTERISTICS OF THE PROGRAMME</u></b>	<b>3</b>
<b><u>4. RESTRICTIONS AND REGULATORY COMPLIANCE</u></b>	<b>4</b>
<b><u>5. REMUNERATION AND CALCULATION.</u></b>	<b>4</b>
<b><u>6. SELF-BILLING AND FISCAL RESPONSIBILITY</u></b>	<b>5</b>
<b><u>7. PROTECTION OF PERSONAL DATA</u></b>	<b>5</b>
<b><u>8. LEGISLATION, JURISDICTION AND COMPETENCE</u></b>	<b>5</b>
<b><u>9. ANNEX I</u></b>	<b>6</b>

## 1.- INFORMATION LEGAL.

**Company Name:** PRESSBROKERS, S.L., hereinafter PRESSBROKERS

**Trade name:** BITNOVO®

BITNOVO® is a trademark owned by PRESSBROKERS registered in Spain under number M3658597.

**Address:** Isla de Cerdeña 1, Bajo, 46023, Valencia, Spain

**VAT NO:** B-98346646

**Registration:** Valencia Companies Register, Volume 9.334, Folio 18, Entry 1, Page V-143.975 Telephone: +34 960 661 265

**E-mail:** info@bitnovo.com

## 2.- OBJECT.

The purpose of this document is to establish the General Conditions that will apply to the BITNOVO® Referral Programme.

## 3.- CHARACTERISTICS OF THE PROGRAMME

The BITNOVO® Referral Program ("Program") is a binding agreement between BITNOVO® and referrers, which allows referrers to refer BITNOVO® services to other persons ("Referrals") and to receive remuneration for such referrals.

In order to acquire the status of referrer and generate links or referral codes, the user must be registered and validated at BITNOVO®, in accordance with the provisions of the [General Conditions of Access and Use for Website and Application Users](#).

Access to and participation in the Programme implies full acceptance of these General Terms and Conditions. Users who do not accept these terms and conditions may not participate in the Programme.

The links or referral codes are unique and are generated for each referrer, who can generate as many codes or links as they wish through the App and the website. In the referral centre, each referrer can monitor the status of their leads and manage their balance.

The Referrer will have full management capacity, without this agreement being understood as the establishment of any labour or commercial relationship with BITNOVO®, and must comply with these general conditions, as well as any other legal obligation, both tax and social security that may be applicable, with the Referrer being solely responsible for such compliance.

The referrer may invite as many referrals as he/she wishes without limit.

## 4. RESTRICTIONS AND COMPLIANCE

Referrers shall not have an employment or business relationship with BITNOVO® and shall not be considered agents or sales representatives of BITNOVO®.

Referrers shall refrain from sending referral codes or links to potential Referrers in countries that BITNOVO does not serve due to regulatory compliance policies.

Referrers must comply with all applicable laws and regulations, including data protection regulations and the law on information society services, and may not send, among others, commercial communications classified as SPAM.

In the event of any breach of any of the conditions set out in this document, or any breach of the applicable legislation, the referrer will lose its status and, therefore, the right to receive the remuneration that may correspond to it, from the moment that BITNOVO® becomes aware of the breach, without the right to make any claim whatsoever for this concept.

Similarly, no Fees shall be paid in the event that BITNOVO® becomes aware, by any means, that the Referrer or Referred has acted fraudulently or in bad faith, in contravention of the provisions of these general terms and conditions, as well as the applicable legislation.

## 5. REMUNERATION AND CALCULATION

Referrers shall earn a remuneration (hereinafter referred to as "Fee") for each Referral who registers with BITNOVO® and makes one or more transactions on the BITNOVO® platform.

Referrers can check their balance in the Referral Centre of the App or in the user panel on the website, and check the rewards earned for each transaction of their referrals.

Fees will be calculated and paid in euros (€) based on the total commission that BITNOVO® earns for the transactions made by each referral.

When the balance generated is equal to or greater than €20, the referrer can transfer it to their Euro Wallet and from there they can make cryptocurrency purchases, withdraw the balance by bank transfer or make a cash withdrawal through our Cash-out service.

Each referrer may receive a maximum remuneration of €2,000 gross for each user he/she has referred.

Each referrer will receive a free NFT.

The referrer's referral status will be maintained for a period of 18 months after the referral's first transaction.

## 6. SELF-INVOICING AND SOCIAL RESPONSIBILITY

The Referrers authorise BITNOVO® to generate a self-invoice for the Fees obtained, including the applicable taxes. The Referrers have a period of five days to check the details of this invoice; if no objection is made within this period, it shall be considered valid for all purposes.

The Referrers shall be solely responsible for the fulfilment of fiscal and social security obligations related to the Fees.

## 7. PROTECTION OF PERSONAL DATA

BITNOVO® and the referrers are obliged to respect the current regulations applicable to the processing of personal data and, in particular, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 applicable as of 25 May 2018 (hereinafter, the "GDPR"), as well as Organic Law 3/2018 of 5 December on the Protection of Personal Data and Guarantee of Digital Rights (LOPDGG).

All in accordance with the provisions of Annex I.

## 8. LEGISLATION, JURISDICTION AND COMPETENCE

These General Conditions are governed by the Spanish legislation in force at the time of their publication.

The parties agree to submit any dispute arising from this contract to the Courts and Tribunals of the city of Valencia, expressly excluding any other jurisdiction that may correspond to them.

## ANNEX I

Within the framework of their contractual relations, the Parties are obliged to respect the regulations in force applicable to the processing of personal data and, in particular, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 applicable as of 25 May 2018 (hereinafter the "GDPR"), as well as Organic Law 3/2018 of 5 December on the Protection of Personal Data and C (LOPDGG).

In accordance with the above, both parties hereby enter into this Annex in accordance with the following,

### **Stipulations:**

#### **One. - The purpose of the processing order.**

By means of these clauses, the Referrer is authorised as data processor to process on behalf of BITNOVO®, in its capacity as data controller, the personal data necessary to provide the service specified hereinafter.

The processing will consist of the management of new customers who are referred. For this purpose, the processor may communicate, including by transmission, collate, collect, record, structure, modify and consult.

#### **Second - Identification of the information concerned**

For the execution of the services derived from the fulfilment of the object of this order, the entity as data controller, makes available to the Referrer, the identification data of the referred customers who have made a purchase or swap at BITNOVO®, in order to keep a good management of their leads.

#### **Third - Duration**

This agreement shall remain in force for the duration of the contractual relationship between the parties.

This contract may also be terminated for the following reasons.

Termination or expiry of the provision of services between the parties; for other causes provided for by law.

In the event of breach by either party of the obligations assumed in this contract, the other party may terminate the contract entirely, without notice or compensation of any kind, and it shall be sufficient to notify the other party of such termination, unless the defaulting party remedies its breach to the satisfaction of the other party within 15 days of the request to that effect being made.

Other grounds provided for by law.

Upon termination of this contract, the data processor must delete any copies of personal data in its possession. However, it may keep the data blocked for the minimum time necessary to deal with possible liabilities that may arise, destroying them securely and definitively at the end of this period.

#### **FOURTH: Obligations of the data processor.**

The data processor and all its staff are obliged 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) To process the data in accordance with the instructions of the data controller. If the processor considers that any instructions are in breach of 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 processing activities of the controller, containing:

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 (hereinafter, DPO).

The categories of processing operations carried out on behalf of each controller.

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.

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

Pseudonymisation and encryption of personal data.

The ability to ensure the continued confidentiality, integrity, availability and resilience of processing systems and services.

The ability to restore availability and access to personal data quickly, in the event of a physical or technical incident.

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 a n 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 overriding 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 operation, this fact must be communicated in advance and in writing to the data controller, one month in advance, indicating the processing operations to be subcontracted and clearly and unequivocally identifying the subcontracting company and its contact details.

The subcontractor, who will also have the status of data processor, is also obliged to comply with the obligations established in this document for the data processor and the instructions issued by the data controller. It is the responsibility of the initial processor to regulate the new relationship in such a way that the new processor is subject to the same conditions (instructions, obligations, security measures, etc.) and the same formal requirements as the initial processor, as regards the proper processing of personal data and the guarantee of the rights of the data subjects. In the event of non-compliance by the sub-processor, the initial processor shall remain fully liable to the controller for compliance with the obligations.

- f) Maintain the duty of secrecy with regard to the personal data to which it has access by virtue of this assignment, even after the end of its object.
- 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 the protection of personal data for persons authorised to process such data.
- j) Assist the controller in responding to the rights that the GDPR provides to data subjects.



In this regard, it is established that the data processor must resolve, on behalf of the data controller, and within the established period, requests to exercise the rights of access, rectification, erasure and objection, limitation of processing, data portability and the right not to be subject to automated individualised decisions, in relation to the data that are the subject of the order.

k) Right to information.

It is the responsibility of the data controller to provide the right to information at the time of data collection.

l) Notification of data security breaches.

The data processor shall notify the data controller, without undue delay, and in any event within a maximum period of 72 hours and via the email that BITNOVO® communicates to it, of any breaches of the 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. Likewise, it shall notify any failure it has suffered in its information processing and management systems that may jeopardise the security of the personal data processed, their integrity or availability, as well as any possible breach of confidentiality as a result of the disclosure to third parties of the data and information accessed during the performance of the contract.

Notification shall not be required where such a breach of security is unlikely to constitute a risk to the rights and freedoms of natural persons.

At least the following information shall be provided:

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.

The name and contact details of the DPD or other point of contact where further information can be obtained.

Description of the possible consequences of the personal data security breach.

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 gradually without undue delay.

The data processor is responsible for communicating data security breaches to the Data Protection Authority (Spanish Data Protection Agency). Likewise, this same figure shall be responsible for notifying, in the shortest possible time, these same notifications to the data controllers.



concerned, in so far as such a violation is likely to pose a high risk to their rights and freedoms.

The communication should be in clear and simple language and should contain, as a minimum:

- Explanation of the nature of the data breach.
  - An indication of the name and contact details of the DPO or other point of contact from whom further information can be obtained.
  - Describe the possible consequences of a personal data security breach.
  - Describe the measures taken or proposed by the controller to remedy the personal data breach, including, where appropriate, measures taken to mitigate possible negative effects.
- m) Support the controller in carrying out Data Protection Impact Assessments, where appropriate.
- n) Support the controller in carrying out prior consultations with the supervisory authority, where appropriate.
- o) Make available to the controller all information necessary to demonstrate compliance with his or her obligations, as well as for audits or inspections carried out by the controller or another auditor authorised by the controller.
- p) Implement security measures in accordance with the risk analysis carried out and, in any case, implement mechanisms to:
- Ensure the continued confidentiality, integrity, availability and resilience of processing systems and services.
  - Restore availability and access to personal data quickly, in the event of a physical or technical incident.
  - Regularly verify, evaluate and assess the effectiveness of the technical and organisational measures implemented to ensure the security of the processing.
  - Pseudonymise and encrypt personal data, where appropriate.
- q) Designate a DPO, if appropriate or legally required, and communicate his or her identity and contact details to the data controller.
- r) Destination of the data.

Delete all personal data upon completion of the processing service commissioned.

Data shall not be destroyed when there is a legal provision requiring them to be kept, in which case they must be returned to the data controller, who shall ensure that they are kept, duly blocked, for as long as such obligation persists.

The return should entail the complete erasure of the data on the IT equipment used by the 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, in accordance with the legally established deadlines for each case. Once the periods indicated have expired, they must be completely destroyed.

#### **QUINTA.- Obligations of the controller**

It is the responsibility of the controller:

- a) The delivery to the data processor of the data referred to in the second clause of this contract.
- b) The performance of a Personal Data Protection Impact Assessment of the processing operations to be carried out by the processor, if applicable.
- c) Carrying out the appropriate prior consultations.
- d) Ensure, prior to and throughout the processing, that the processor complies with the GDPR and other applicable regulations.
- e) Overseeing treatment, including carrying out inspections and audits.