NON-DISCLOSURE AGREEMENT

This **Non-Disclosure Agreement** (the "**Agreement**") is entered into as of the date of the last signature hereto (the "**Effective Date**") byand between Bytro Labs GMBH (together with its respective employees, officers, directors and advisors, "**Bytro Labs**") and the individual(s) set out in the signature block below ("**Recipient**"). Bytro Labs and the Recipient are each referred to as a "**Party**" and collectively the "**Parties.**"

1. Confidential information. As used in this Agreement, "**Confidential Information**" means any nonpublic and/or proprietary information related to Bytro Labs that: (a) if disclosed in writing, is labeled as "confidential" or "proprietary"; (b) if disclosed orally, is designated confidential at disclosure; (c) by its nature and/or the circumstances of its disclosure, should be reasonably considered as confidential and/or (d) any personal information acquired and used in the role of the service and accordance with the purpose. Confidential Information may include, without limitation, information respecting a Bytro Labs's technologies, pricing lists, pricing plans, customer information, user information, account information, research, know-how, trade secrets, strategic information, business plans, technical information, policies, and other proprietary information which Bytro Labs takes reasonable efforts to keep secret.

2. Purpose. The Recipient may use Confidential and personal Information in their role as volunteer and for the purpose of providing services to Bytro Labs ("**Purpose**"). In connection with the Purpose, Bytro Labs may disclose Confidential Information to Recipient. In order to prevent unauthorized disclosure or use of such Confidential Information, the Parties have entered into this Agreement.

3. Use of Confidential Information.

3.1. The Recipient shall keep Confidential Information strictly confidential and not disclose such Confidential Information to any third party without Bytro Labs's prior consent. The Recipient shall treat such Confidential Information with a reasonable degree of care and as benefiting the sensitivity of the information.

3.2. The Recipient may only access systems and use information they receive for the Purpose. The Recipient must maintain regulatory requirement and standards when processing the Confidential information and maintain security and secrecy in accordance with the measures set forth in all governing documents by Bytro and the information found in Appendix 1.

3.3. The Recipient must comply with applicable data protection laws and regulations and is, in particular, prohibited from exploiting the Service and/or extract, use (other than as strictly required for the Service) or otherwise disclose any personal information the Recipient gains access to through the Service and hereby agree to adhere to relevant data protection laws and regulations, including but not limited to the German Federal data protection Act.

3.4. The Recipient may disclose the Confidential Information to third parties only as permitted by Bytro Labs in writing and then on a strictly "need-to-know" basis.

3.5. Confidential Information does not include information that the Recipient can reasonably prove (a) was known to the Recipient prior to the time of disclosure by Bytro Labs; (b) was or becomes publicly known through no fault of, or breach of the Agreement by, the Recipient; or (c) was independently developed by the Recipient without reference to or use of the Confidential Information.

4. Right to Notice. In the event Recipient receives a request to release Confidential Information pursuant to a court order, subpoena, or request from any other governmental authority, or the Recipient is otherwise obliged to disclose Confidential Information, Recipient shall, where possible, provide Bytro Labs with prompt written notice in order to permit Bytro Labs to either consent to the disclosure or seek a protective order or other appropriate remedy. Nothing in this Agreement shall prevent the Recipient from disclosing information which it is obliged to disclose pursuant to law. Recipient shall limit the disclosure of Confidential Information to the greatest extent possible.

5. Return of Confidential Information. Upon Bytro Labs's request, the Recipient shall promptly return or, at Bytro Labs's option, destroy all documents or other recorded means containing Confidential Information and any other documents, specifications, data or information of any nature whatsoever based on or relating to Confidential Information. Upon the request of Bytro Labs the Recipient shall promptly certify in writing that such destruction has been completed.

6. No License. Any and all rights to Confidential Information, including but not limited to copyright, trademarks, patents and any other intellectual property rights, shall remain the property of Bytro Labs. No license to or in any of the Confidential Information is hereby granted directly or indirectly or implied in any way whatsoever. This Agreement imposes no obligation on either Party to proceed with any business transaction or agreement and does not create any agency or partnership of any kind between the Parties.

7. Termination. Bytro Labs may terminate this Agreement by written notice to the Recipient. Recipient may terminate this Agreement by giving Bytro Labs no less than 14 days' written notice. Except as set out in Section 3.5, the Recipient's confidentiality obligations will survive the termination of this Agreement.

8. Compliance with Laws. The Recipient confirms it is aware of the applicability of German and European securities, laws and regulations and will adhere to the same when performing the Services.

9. Amendments. Any amendments to this Agreement must be made in writing and signed by both Parties in order to be valid.

10. Counterparts; No Assignment. This Agreement may be executed in counterparts, and via facsimile and/or .pdf. Neither Party may assign or transfer this Agreement without the written consent of the other Party, not to be unreasonably withheld.

11. Governing Law. This Agreement shall be governed and construed by German law, excluding any conflicts of laws principles. Any dispute, controversy or claim arising out of or in connection with this Agreement, or the breach, termination or invalidity thereof, shall be finally settled by the courts of Hamburg (or any other court mandated by applicable mandatory law).

12. Equitable Relief. The Recipient acknowledges that breach of this Agreement may cause irreparable harm to Bytro Labs. Therefore, in addition to any other remedies available to it, Bytro Labs may seek injunctive relief in the event of any breach or alleged breach of this Agreement without proving actual damages.

13. Notices. Any notice hereunder will be effective upon receipt and must be given in writing and delivered to the other party through email or via designated communication method (as separately notified by the Parties).

14. Supersedes Prior Agreements. This Agreement shall supersede and replace all prior non-disclosure agreements between Bytro Labs and the Recipient.

***

BYTRO LABS GMBH

BY: ppa Julian Werner

TITLE: Director Marketing

DATE: 2024-02-06

BY: Christopher Lörken

TITLE: Managing Director

DATE: 2024-02-06

RECIPIENT:

BY:____________________________

Place: ____________________________

DATE: ____________________________

Appendix 1

Fact sheet about the obligation to data secrecy

Unauthorized persons should not have access to personal data. Personal data is protected by the German Federal Data Protection Act and the General Data Protection Regulation. You are responsible within the scope of your function for our company to keep data confidential and process as instructed. You are responsible that all the user data that you have been entrusted with is only being processed (saved, changed, transmitted, locked, deleted) or used in the scope of your work. Abuse of data or any other unauthorized action is prohibited.

You act unauthorized if you gather, use and process data against the purpose connected to your occupation. Especially you are personally responsible for the following:

- The data you have been entrusted with is kept under wraps if you are not directly working with it.

- your device for data processing, applications, and passwords, which are used for your work are not accessible to unauthorized persons,
- No information is removed, accessed or disclosed through non-approved systems.

- no longer used data storage devices which contain personal data are destroyed accordingly to the German data protection law, so an abusive further use is not possible.

- All other instructed, company internal technical and organizational measures are adhered to.

Explanation about Data protection act

Purpose of data protection act
The purpose of the data protection act is to protect every single person from having their personal rights negatively affected. Every person concerned should decide on their own who has access to which personal data and for which purpose.

Explanation of terms

- **Personal data** include particulars about personal (for example: name, birthday, age, civil status, citizenship, job, criminal records, habits) or material (for example: income, taxes, insurances, car ownership, account number, credits, deposits, properties) circumstances of a specific or identifiable natural person (affected person). Personal data about deceased persons are not protected by the data protection act.
- **Special types of personal data** are information about the racial and ethnic origin, political opinions, religious or philosophic convictions, membership in a trade union, health or sexual life.
- **Collecting data** is acquiring data about the affected person.
- **Types of data processing** are saving, changing, transmitting, disabling and deleting personal data.
- **Saving** means acquiring, gathering or keeping personal data on a device for the purpose of processing or usage of the data.
- **Changing** personal data refers to content-related rearranging of saved personal data.
- The disclosure of saved personal data or data that has been obtained by processing personal data to a third party or allowing a third party to have insights or access to this data is declared as **transmission**.
- **Blocking** takes place when personal data is tagged to avoid or limit further processing or usage.
- Blurring personal data is declared as **deletion**.
- **Usage** describes every use of personal data, insofar as it is not a form of processing.
- **Anonymization** is changing personal data to the extent that any personal or material particulars can not not be associated with a specific or identifiable natural person without an excessive effort in terms of time, costs and manpower.

- **Pseudonymization** describes the exchange of names and other identifying features to hinder the determination of the affected person.
- **Responsible Institution** is every person or institution which collects, processes or uses data for themselves or orders others to do so.
- **Receiver** describes everyone that has access to data.
- **Third party** is every person beyond the responsible institution - not the affected person nor those people or institutions in the inland, in another EU member state or in another state party with the European Economic Area which process and use personal data when ordered.
- **Mobile personal storage media to process data** are data devices, that are handed over to the affected persons with which they will be able to process personal data.

Legitimacy of data handling
Collecting, saving, changing or transmitting personal data or their usage is only allowed if it aligns with the regulations of the data protection act or another legal regulation or if the affected person approved it.

If an authorization is given by a regulation an approval of the affected person is not needed. If the regulation is not given, the approval of the affected person is mandatory. The approval must be given in writing (in specific cases electronical approval is enough). The person affected is to be informed about the meaning of their approval, especially the purpose of the data usage and who will receive those.

Rights of the affected person
Every affected person has the right to receive information about the personal data saved, who has access to it and the purpose of the data storage.

The affected person can in specific cases demand the deletion of the data or decline collecting, process and usage of their personal data.

A requirement to make use of their rights is that the affected person knows that data about them is saved. For this reason every responsible institution is required to inform the affected person. The duty of notification is no longer required if the affected person received notice in another way, the notification requires an excessive effort or saving and transmitting of the personal data is intended by law regulations.

The affected person can make use of their rights and claim for damages and get in contact with the responsible controlling authority at any time.

Duty to protect the data secrecy
According to the data protection act we have to introduce you to the data secrecy. Data secrecy means that it is forbidden to collect, process or use personal data unauthorized. Data secrecy remains even after resignation.

Part of the data handling is everyone who collects, processes and uses personal data.

Violation of the data secrecy can be punished according to the regulations of the data protection act with deprivation of liberty or financial penalty.

Statutory offence
Specific actions which violate the data secrecy will result in punishment according to the German criminal code (“Strafgesetzbuch”). Especially following statutory offences: § 303a (“data manipulation”), § 303b (“computer sabotage”), § 202a (“Spying out of data”) and § 263a (“computer fraud”). People who change or remove data illegally, disturb the procedure of data processing, collect data from unknown data systems or share them with unauthorized person or someone who damages others’ property by allowing illegal influence during the process of data handling.

Requirements under data protection law
This section specifies the responsibilities of the parties in terms of data-protection law in regards to technical and organizational requirements to secure the data of Bytro Labs from misuse and loss, which are regulated by the requirements of the German Federal Data Protection Act (§ 9 BDSG) and German General Data Protection

Regulation (Art 24, 32 DSGVO) This includes especially:

- Refuse unauthorized persons access to data processing facilities, with which personal data is processed and used (entry control),

- prevent that data processing systems can be used by unauthorized persons (access control),

- take care that authorized people only have access to the personal data which is covered by their responsibilities and that data can not be read, copied, changed or removed by unauthorized persons during processing, using and saving them (user access control),

- take care that personal data can not be read, copied, changed or removed by unauthorized persons during the electronic transmission or storage on data storage devices and be aware of the time when a transmission of personal data is taking place (control of transmission),

- take care that every action (entering, changing, deleting) with personal data can be checked afterwards. Who processed personal data when and how (input control),

- take care that personal data which is processed on behalf of others is only processed in the way instructed and needed to complete the respective task. (order supervision),

- take care that all personal data is protected against accidental destruction and loss (availability check),

- assure that data used for different purposes can be processed separately (separation control),

- the pseudonymization and encryption of personal data,

- the ability to permanently secure the confidentiality, integrity, availability and capacity of the system and services in regards to processing data,

- the ability to quickly restore the access to personal data in case of a physical or technical incident,

- a procedure to constantly monitor, evaluate and rate the efficiency of the technical and organizational measures to ensure the security of processing.

- The technical and organizational measures underlie technological progress and further development. Therefore the moderator is allowed to implement alternative, suitable measures. The current security level must not be undercut due to these alternative measures. Fundamental changes are to be documented.