Agreement on Processing

Version 3.0

concluded between

1. You

(hereinafter referred to as **"principal"** or **"controller"**)

on the one hand, and

2. Pinpoll GmbH, Hopfengasse 3, 4020 Linz, registered in the commercial register of the regional court in Linz under the registration number FN 433631 v

(hereinafter referred to as **"agent"** or **"processor"**)

on the other hand

(both 1 and 2 together referred to as **"parties"**)

as follows:

1. Preamble

1.1 The regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 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, OJ 04.05.2016 L 119/1 (shall be referred to as **"GDPR"**) is directly applicable since May 25, 2018 and binding in its entirety. In order to implement the GDPR, the law on the protection of natural persons with regard to the processing of personal data (BGBl I 2018/24, shall be referred to as "DSG") has been adopted with the "Datenschutzanpassungsgesetz 2018" that entered into force on May 25, 2018.

1.2 The controller and the processor have to conclude an "Agreement on Processing" according to Art 28 GDPR. The parties meet that obligation with the given agreement.

1.3 The given agreement explicitly refers to the GDPR as its legal basis. The relevant clauses of the DSG shall apply mutatis mutandis. Provided that the DSG contains divergent clauses, explicit reference will be made.

2. Subject

2.1 The use of the software solutions provided by Pinpoll in order to gather and analyse data of users by the principal shall be based upon the terms and the data protection declaration of the agent in their current version, available at https://pinpoll.com.

2.2 This agreement refers to all activities by which the agent processes personal data that are provided by the principal.

2.3 The gathered personal data by the agent shall be derived from clause 3 of the data protection declaration.

2.4 Data subjects of the processing shall be, on the one hand, the principal himself and, on the other hand, individuals who use services of the principal and, therefore, are affected by the software solutions of the agent.

2.5 The nature and purpose of the processing shall be derived from clauses 3 to 5 of the data protection declaration.

3. Duration

This agreement shall enter into force as from creating a Pinpoll account and shall be concluded for an indefinite period of time.

4. Rights and Obligations of the Principal

4.1 The principal as controller shall be obliged to ensure compliance with data protection regulations according to the GDPR and other relevant rules with regard to data protection. The principal shall be obliged in particular to respect the principles relating to the processing of personal data pursuant to Art 5 GDPR and to guarantee the rights of the data subject, especially pursuant to Art 12 – 22 GDPR.

4.2 The principal has the right to give instructions to the agent according to Art 28 para 3 lit a and Art 29 GDPR. The principal shall give the instructions in written form.

4.3 The principal shall be entitled to demand compliance from the agent with regard to the technical and organisational safety measures to be taken by the agent under the GDPR within the meaning of clause 6 by submission of appropriate evidence.

5. Rights and Obligations of the Agent

5.1 The agent as processor shall be obliged to ensure compliance with data protection regulations according to the GDPR and other relevant rules with regard to data protection.

5.2 The agent shall guarantee that the principal is able to meet its fulfilment with regard to the rights of data subjects pursuant to Art 12 – 22 GDPR. In particular, the agent shall adopt appropriate technical and organisational safety measures within the meaning of clause 6 in order to support the principal with regard to its duty to respond to requests of data subjects.

5.3 The agent shall be obliged to support the principal – taking into account the information available to the agent – with regard to the measures of data security according to Art 32 GDPR, in case of necessary notification to the authority according to Art 33 GDPR, in case of communications of data subjects according to Art 34 GDPR, with regard to the implementation of a data protection impact assessment according to Art 35 GDPR as well as with regard to consultation of authorities according to Art 36 GDPR.

5.4 The agent allows for and contributes to audits – including inspections – conducted by the principal or another auditor managed by the principal.

5.5 The agent shall immediately inform the principal if, in his opinion, an instruction according to clause 4.2 of this agreement on processing infringes the GDPR or other relevant data protection provisions.

6. Technical and Organisational Safety Measures

6.1 The agent shall ensure the adoption of the safety measures required to fulfil the proper implementation of the commissioned works. This also applies to the engagement of a sub processor according to clause 7 of this agreement. The agent and the sub processor shall adopt appropriate technical and organisational measures to ensure adequate protection of personal data that meet the requirements of the GDPR, especially of Art 32 GDPR (details may be taken from Annex ./1).

6.2 The technical and organisational safety measures required are subject to technical progress and advancement. Hence, the agent shall be entitled to adopt alternative appropriate measures.

6.3 In this context the agent refers to the terms and certifications in their respective and current versions of its sub processor according to clause 7.2, available at https://www.microsoftvolumelicensing.com/Downloader.aspx?DocumentId=12826 and https://www.microsoft.com/en-us/TrustCenter/Compliance/iso-iec-27018.

6.4 The principal is aware of the implemented technical and organisational measures by the agent. The principal bears the responsibility that these measures provide an adequate level of protection with regard to the risks of personal data should be processed.

7. Sub Processor

7.1 The agent shall be entitled to engage other processors (hereinafter referred to as **"sub processors"**) for the processing of data of the principal. The agent shall remain liable to the principal for the performance of the sub processor's obligations.

7.2 The principal gives its irrevocable consent to the engagement of Microsoft Corporation, Redmond, WA 98052-6399 USA as sub processor by the agent. The consent can be withdrawn if, with regards to the involvement of Microsoft Corporation as a subcontractor, the requirements according to Art 45 ff GDPR no longer exist.

7.3 The agent shall inform the principle at least 1 (in words: one) month prior to the planned engagement of another processor and shall announce the name and address of the sub processor.

7.4 The principal shall be entitled to object to the engagement of the sub processor in writing within 14 (in words: fourteen) days of the receipt of information. In this case, the agent und the principle shall jointly decide upon their further cooperation.

8. Data Erasure

8.1 The agent shall be entitled to store personal data (especially data carriers and documents) provided in the course of the processing as long as it is necessary to carry out the respective processing.

8.2 Upon demand of the principal and upon termination of the given agreement, the agent shall be obliged to erase or destroy in conformity with the relevant data protection regulations all personal data provided in the course of the processing (especially data carriers and documents) promptly, but at least within 14 (in words: fourteen) days from the demand and instruction of the principal, or after fulfilment of the contractual obligations. Once erased or destroyed, Pinpoll will confirm this in writing.

9. Secrecy

9.1 The parties, their organs, representatives, employees or proxies shall be obliged to treat as confidential and not to disclose to a third party all mutually notified targets, data, documents, results of own or common research or other information upon research or operational nature during the term of validity and within an unlimited period of time after the termination of the given agreement. The contracting parties undertake to ensure that their organs, representatives, employees or proxies assume the aforementioned duties.

9.2 The following especially, but not exclusively shall be treated as confidential:

9.2.1 Facts and information upon commercial operations;

9.2.2 Products;

9.2.3 Information upon means of procurement.

10. Termination

10.1 This agreement shall be terminated if the Pinpoll account is erased by the principal or by the agent in the course of measures of data clearing, provided that the relevant account has not been used for 12 (in words: twelve) months or in case of a serious or repeated breach of the terms.

10.2 Both of the parties shall be entitled to terminate this agreement without notice if the insolvency procedure has been opened against the other party, or the request for the opening of the insolvency procedure has been rejected due to insufficient resources or the conditions for the opening of such a procedure or for the rejection of such a request are fulfilled or the other party ceases payments, unless mandatory law permits the latter.

10.3 Both of the parties shall be entitled to terminate this agreement 2 (in words: two) months after:

10.3.1 the other party is no longer able to fulfil this agreement for whatever reason;

10.3.2 the other party persistently violates its obligations arising from this agreement.

11. Waiver

The parties waive to avoid this agreement, to demand its adjustment or to demand that it is void.

12. Miscellaneous

12.1 Any amendment or supplement to or modification of this agreement, including this provision, shall be valid only if made in writing. If there exists any other oral agreement, it shall be void.

12.2 In the event that any provision of this agreement should become void or unenforceable, the other provisions of this agreement remain in full force and effect. The void or unenforceable provision shall be deemed to be replaced by a valid, enforceable and mutually acceptable provision that comes as close as possible to the economic result of the void or unenforceable provision. This applies mutatis mutandis to gaps in this agreement.

12.3 All disputes or claims arising from or in connection with this agreement shall be settled at the local court of Linz. This declaration shall be governed by and interpreted in accordance with the laws of Austria, excluding the principles of conflict of laws.

12.4 In case of doubt, the German version prevails.

Annex ./1 – Technical and Organisational Safety Measures

PART A

Part A of this annex describes which technical and organisational safety measures the agent takes.

Confidentiality

This section describes the measures the agent takes to ensure protection against unauthorized disclosure of information:

- Physical Access Control: Protection against unauthorized access to the building and office through multiple locking and burglar-proof door locking systems, documentation of key allocation;
- Data Access Control: Protection against unauthorized system access through strong passwords (including a corresponding policy), automatic locking mechanisms, encryption of data carriers (FileVault);
- Data Usage Control: No unauthorized reading, copying, changing or removing within the system, standard processes for assigning authorizations, logging access, periodic review of the authorizations granted, including deactivation and deletion of accounts (especially those with administration rights);

Data Integrity

This section describes which measures the agent takes to prevent unauthorized reading, copying, modification or removal of data:

- Transfer Control: No unauthorized reading, copying, changing or removing in the case of electronic transmission or data transport through encryption, virtual private networks (VPN), documentation of certificate allocation, as well as electronic signature;
- Input Control: Logging and document management to determine whether and by whom personal data has been entered, changed or removed in data processing systems;

Availability and Resilience

This section describes the measures the agent takes to prevent accidental or deliberate destruction or loss of data:

- Availability Control: Protection against accidental or deliberate destruction or loss, backup strategy (both online / offline and on-site / off-site), virus protection, firewall, air conditioning of the premises, standard processes in the event of employee changes / releases;
- Rapid recovery through high availability;

Procedures for Regular Testing, Assessing and Evaluating

This section describes the organisational measures the agent takes to maintain a high level of data protection:

- Agreement upon strict non-disclosure contracts with all employees;
- Data protection management, including regular employee awareness training;
- CRM-based incident response management (ticketing, automated workflows);
- Order control (cf. PART B): No data processing according to Art 28 GDPR without corresponding instructions from the client through clear contract drafting, formalized order

management, strict selection of the order processor (ISO certification, ISMS), obligation to provide prior conviction, follow-up controls;

PART B

The agent last convinced themselves on February 1, 2021 that their sub-processor Microsoft is taking sufficient technical-organisational measures.

These are described in detail by Microsoft in **Appendix A - Security Measures** of document https://www.microsoftvolumelicensing.com/Downloader.aspx?DocumentId=18030.

The current version of this document can be downloaded in several languages here:
https://www.microsoftvolumelicensing.com/DocumentSearch.aspx?Mode=2&Keyword=DPA