iP.1 Data Processor Agreement

Data Controller (DC):

Customer

Data Processor (DP):

IP.1 Networks AB, 556671-1536

1. Background and scope

The Data Controller is referred to as DC in this document. The parties have entered into an agreement whereby IP.1 Networks AB undertakes to perform services under the agreement "Service Agreement" on DC's behalf. In performing these services under the Service Agreement, IP.1 Networks AB will process personal data for DC's behalf. Accordingly, IP.1 Networks AB will act as a personal data processor, DP, for DC in the performance of the relevant services, which is the personally responsible person for the personal data to be processed.

2. Objects of the personal data

IP.1 Networks AB may only process personal data for the purposes stated in the Service Agreement or written additional agreements that refer to this Agreement and not for any other purpose than what is necessary for the performance of the Service Agreement.

3. Subcontractor

IP.1 Networks uses cloud services within the EU as a subcontractor. IP.1 Networks AB may not, without written consent, provide personal information to be processed by a subcontractor. If a general consent is given, IP.1 Networks AB shall inform DC of any plans to change or hire new subcontractors. DC shall promptly object to such changes, but no later than one week from IP.1 Networks AB announced that the change will occur.

If DC opposes changes, personal data may not be disclosed and the services shall be performed by IP.1 Networks AB on its own or alternatively by a previously approved sub-party.

IP.1 Networks AB is responsible for entering into written agreements with subcontractors.

4. Conditions for processing personal data

For IP.1 Networks AB's processing, the following applies.

IP.1 Networks AB

a) may only process personal data on documented instruction from the DC, including in the case of transfer of personal data to a third country or international organization, unless this process is required by European Union law or national law. In such case, IP.1 Networks AB shall inform the DC of the legal requirement before processing the data, unless such information is prohibited by reference to an important public interest under this right,

b) shall ensure that all personnel authorized to process personal data have taken it upon themselves to observe confidentiality or are subject to appropriate statutory professional secrecy,

c) shall take all security measures in connection with the processing of personal data in accordance to Article 32 of the General Data Protection Regulation,

d) shall respect the terms and conditions for the use of the subcontractors in accordance with item 3 above,

e) in view of the nature of the processing, assist the DC through appropriate technical and organizational measures, to the extent that this is possible, so that the DC can fulfill its obligation to respond to the request for the exercise of the data subject's rights in accordance with Chapter III of the General Data Protection Regulation,

f) shall assist the DC to ensure that the obligations under Articles 32-36 of the General Data Protection Regulation are complied with (regarding information to the registered person subject to a personal data incident and the notification of a personal data incident to the regulatory authority), taking into account the type of processing and the information available to IP.1 Networks AB,

g) depending on what the DC chooses, delete or return all personal data to the DC after the provision of the processing services has been terminated, and delete existing copies unless the storage of personal data is required by European Union law or national law, and

h) shall provide the DC with all information required to demonstrate compliance with the obligations set out in this article, as well as enable and contribute to audits, including inspections conducted by the DC or by another auditor authorized by the DC.

Furthermore, IP.1 Networks AB commits to keep records of the processes and to cooperate with the regulatory authority and make this registry available to the regulatory authority.

IP.1 Networks AB will assist the DC, as required and upon request, with the fulfillment of the obligations arising from the conduct of consequence analysis regarding data protection and prior consultation with the regulatory authority.

5. Safety measures

IP.1 Networks AB shall restrict access to personal data to personnel who need such access to perform their duties.

IP.1 Networks AB will ensure that personal data are not processed in violation of the provisions of current legislation, etc. regarding data protection for personal data such as data protection regulation and data inspection regulations. IP.1 Networks AB shall take appropriate technical and organizational measures to protect personal data from unauthorized access, destruction and modification.

IP.1 Networks AB undertakes to inform the DC immediately if an instruction violates the General Data Protection Regulation or against other personal data protection provisions.

IP.1 Networks AB and DC are committed to, taking into account the latest developments, implementation costs and the processes' scope, context and objectives and the risks, of varying degrees of probability and severity, of people's rights and freedoms, take appropriate technical and organizational measures to ensure a level of safety appropriate to the risk, including, where appropriate

a) pseudonymization and encryption of personal data,

b) the ability to continually ensure the confidentiality, integrity, availability and resilience of the processed systems and services,

c) the ability to restore availability and access to personal data in a reasonable time frame when a physical or technical incident has occurred,

d) a procedure to periodically test, investigate and evaluate the effectiveness of the technical and organizational measures that will ensure the safety of the process.

In assessing the appropriate level of security should have particular regard to the risks that the process involves, in particular, from the accidental or unlawful destruction, loss or alteration or unauthorized disclosure of, or unauthorized access to personal data transmitted, stored or otherwise processed.

The DC and IP.1 Networks AB shall take measures to ensure that any individual who performs work in the DCs or IP.1 Networks AB's supervision, and who has access to personal data, only will process those on the instruction from the DC, if not the European Union law or the national law of the Member States obliges him or her to do so.

6. Privacy Incidents

IP.1 Networks AB shall notify the DC without unnecessary delay after having been informed of a personal data incident. The notification shall describe the nature of the personal data incident, including, if possible, the categories of and the approximate number of registered people involved, as well as the categories and the approximate number of personal data items concerned. If, and to the extent, that it is not possible to provide the information simultaneously, the information may be provided in parts, without unnecessary further delay.

IP.1 Networks AB shall assist the DC and provide documentation of all personal data incidents, including the circumstances surrounding the personal data incident, its effects and the corrective actions taken.

7. Contacts with third parties

If a third party (eg authority other than the supervisory authority or any other person) addresses IP.1 Networks AB with a request for information regarding the processing of personal data, IP.1 Networks AB shall forthwith forward such a request to DC.

IP.1 Networks AB is not entitled to represent DC against third parties in the processing of personal data unless DC expressly acknowledges this. DC will reimburse IP.1 Networks AB for costs, etc. which may arise due to the fact that IP.1 Networks AB does not provide information about the processing under this paragraph.

8. Professional secrecy

IP.1 Networks AB, and its employees and sub-consultants, have confidentiality for all personal data processed unless otherwise agreed in writing with DC. Confidentiality also does not concern the data subject regarding their own personal data or for information that is generally known.

9. intellectual property rights

All intellectual property rights to the personal data are held by DC or the registered person. IP.1 Networks AB has a non-exclusive right to use the personal data and possibly intellectual property rights attached thereto solely for the performance of its obligations under the Service Agreement.

10. Responsibility

If a registered or other third party claims a claim against DC due to the processing of personal data by IP.1 Networks AB, IP.1 Networks AB shall compensate DC for any claims arising from IP.1 Networks AB failing to comply with this agreement. The compensation is limited to a maximum of half (½) of the Swedish Price Base Amount (Prisbasbelopp).

If a registered or other third party claims a claim against IP.1 Networks AB due to DC's personal data processing instruction, DC shall compensate IP.1 Networks AB for such requirements, but not if IP.1 Networks AB should have notified DC that processing is in violation of current data protection rules.

Any DC or DP involved in the processing of personal data may be held liable for the entire damage to the registered person. However, if they are joined in the same legal proceedings in accordance with the national

law of the Member States, compensation may be distributed according to the responsibility of each DC or DP for the damage caused by the process, provided that the registered person is insured for full and effective compensation. Any DC or DP who has paid full compensation may then initiate recovery procedures against other DC or DP involved in the same process. However, the right of subrogation between DC and IP.1 Networks AB is limited as above.

11. Deletion

IP.1 Networks AB is, after termination of the Service Agreement, required to delete all personal data processed for DC, unless previously agreed upon. IP.1 Networks AB is obliged, in connection with the termination of the Service Agreement, to return processed data in appropriate format to DC.

12. Changes and additions

Changes or additions to this Agreement shall be in writing and signed by both parties to be considered valid.

13. Term and Termination

This Agreement enters into force when signed by both Parties. The agreement expires when the Service Agreement expires. However, paragraph 8 shall continue to apply for one year after the termination of the contract.

14. Dispute

Disputes arising from the agreement shall primarily be resolved through good faith negotiations between the parties. Swedish law is applicable to the contract. Disputes arising in connection with this agreement shall be finally assessed in the general court of Skaraborg District Court (Skaraborgs Tingsrätt).

By using our Services or otherwise by interacting with us, you agree to this Data Processor Agreement.