Annex to the Terms and Conditions between Proxyclick and the Client

-

Data Processing Agreement

Between:

the Client,

hereinafter called the “Client” or the “Controller”

And:

Proxyclick,

hereinafter called “Proxyclick” or “Processor”

Hereinafter independently referred to as "Party" and collectively referred to as "Parties".

The Parties have entered into an agreement to establish the terms and conditions of the provision of visitor management services (the “Services”) by Proxyclick to the Client (the “Agreement”). In the performance of this Agreement, Proxyclick will be processing Personal Data on behalf of the Client. This Data Processing Agreement (“DPA”) details the conditions under which Proxyclick will perform these processing activities. It forms an integral part of the Agreement.

The Parties hereby agree as follows:

1. Definitions

All capitalized terms in this DPA will have the meaning as defined by the applicable Data Protection Legislation, unless otherwise stated in this section or unless the context requires otherwise:

1.1. “***Data Protection Legislation***” shall mean (i) prior to 25 May 2018, the European Directive 95/46/EC, the Belgian Data Protection Act of 8 December 1992, and other national laws and regulations applicable to the Parties which relate to or impact on the processing of Personal Data; (ii) as of 25 May 2018, the 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 (General Data Protection Regulation), the Belgian national data protection laws, and, if applicable, any other national law or regulation applicable to the Parties concerning the processing of Personal Data;

1.2. “***Data Subject***” means the identified or identifiable natural person who uses

Proxyclick's Services, where an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

1.3. "***Personal Data***", any information relating to a Data Subject;

1.4. "***Processing***" means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;

1.5. "***Controller***" (or "Data Controller") means the entity which determines the purposes and means of the Processing of Personal Data;

1.6. "***Processo***r" (or "Data Processor") means the entity which Processes Personal Data on behalf of the Controller;

2. Scope and Objectives of the DPA

2.1. This DPA regulates the measures taken by the Parties in order to protect Personal Data processed in the performance of the Agreement. The Processor shall process Personal Data on behalf of the Controller.

2.2. Proxyclick shall only process Personal Data on behalf of, and in accordance with documented instructions of the Controller including with regard to transfers of Personal Data to a third country or an international organization, unless required to do so by Union or Member State law to which the Processor is subject; in such a case, the Processor shall inform the Controller of that legal requirement before Processing, unless that law prohibits such information on important grounds of public interest. Such processing shall be in accordance with this DPA and Data Protection Legislation. The Controller shall be solely responsible for complying with its obligations under the applicable Data Protection Legislation, including, but not limited to, the lawfulness of the transmission to Proxyclick and the lawfulness of the processing.

2.3. Any documented instruction by the Controller to Proxyclick in relation to the processing (hereinafter a "**Processing Instruction**") shall be defined in the Agreement or this DPA. Modifications to the Processing Instruction are subject to a mutual written agreement.

2.4. The Controller has defined that the following data categories will be collected, processed and used by the Processor under the Agreement:

- For employees of the Controller:
  - First and last name
  - E-mail address
  - Mobile phone number

- For visitors of the Controller:
  - First and last name
  - All other fields are optional and can be activated (or not) by the Controller: e-mail address, phone, picture, signature, company

name...

3. General principles

3.1. The Processing of Personal Data under the Agreement is guided by the following general principles to be respected by all Parties:

3.1.1. Respecting privacy and protection of Personal Data;
3.1.2. Principle of prior informed consent: whenever applicable Data Protection Legislation requires to obtain the consent of Data Subjects; the necessary consent of the Data Subjects will be requested before collecting Personal Data;
3.1.3. Proportionality: the Parties will limit the Processing of Personal Data to what is useful and relevant given the intended purpose of the processing;
3.1.4. Minor of age protection: the Parties undertake to comply with the obligations concerning the protection of minors as set forth by applicable Data Protection Legislation and applicable law.

3.2. All Parties commit to process any Personal Data in accordance with the principles set out above, as well as to minimize repetitions of data (data minimization), and not to keep any Personal Data longer than necessary for the purpose.

4. Rights and Obligations of Controller

4.1. Notwithstanding the provision of article 5.5, the Controller is responsible for the assessment of the legitimacy of the data processing in accordance with Data Protection Legislation.

4.2. The Controller shall issue all orders to the Processor in written form. Any changes to the software and applications of the Processor going beyond mere technical changes and to the extent that they substantially change the object or method of the Processing shall be mutually agreed in writing. Any changes required as a consequence of applicable Data Protection Legislation will be agreed upon in good faith in writing and within the deadlines set forth by applicable Data Protection Legislation.

4.3. The Controller shall inform the Processor without delay should he notice any mistakes or irregularities with respect to the Processing of Personal Data.

4.4. The Controller shall keep confidential any and all kinds of proprietary business information of the Processor which is received as a result of this DPA. The Controller is entitled to disclose the security measures taken to Data Subjects and third parties, without disclosing proprietary business information of the Processor.

5. Rights and Obligations of the Processor

5.1. The Processor shall process the Personal Data in accordance with the Agreement, this DPA and the Data Protection Legislation unless required to do so by Union or Member State law to which the Processor is subject. In that case, the Processor shall inform the Controller of that legal requirement before Processing, unless that law prohibits such information on important grounds of public interest or otherwise.

5.2. The Processor shall assist the Controller in ensuring compliance with the obligations pursuant to applicable Data Protection Legislation (in particular articles 32 to 36 of the General Data Protection Regulation when it will apply) taking into account the nature of Processing and the information available to the Processor.

5.3. The Processor shall correct, delete or block the access to the Personal Data on the instruction of the Controller.

5.4. The Processor shall make available to the Controller all information necessary to demonstrate compliance with the obligations laid down in article 28 of the General Data Protection Regulation, and allow for and contribute to audits, including inspections, conducted by the Controller or another auditor mandated by the Controller. The Processor authorizes the Controller to take any reasonable measures to inspect the Processor's compliance with applicable Data Protection Legislation as well as his compliance with the Controller's instructions.

5.5. The Processor shall inform the Controller if he concludes that an instruction of the Controller may violate applicable Data Protection Legislation. In this case, the Processor may interrupt the relevant processing until instructions are confirmed or changed by the responsible person of the Controller.

5.6. If the Processor receives a request for information or any correction, deletion, blocking from the Data Subjects, he shall transfer such request to the Controller and shall support the Controller in the handling thereof. The Parties agree that the Processor can be in direct contact with the Data Subjects to provide technical support.

5.7. The Processor shall promptly inform the Controller in the event of substantial disruption of the Services or infringements of relevant Data Protection Legislation, including any breach of privacy or security in relation to the Processing arising from the Processor and or its employees. In view thereof, the Controller commits to subscribe on the Proxyclick platform (http://status.proxyclick.com) to receive status updates.

5.8. The Controller authorizes the Processor to use Personal Data of Data Subjects when it is aggregated or anonymized for the purpose of improvement of the Services and research and development. In such form, the data is no longer Personal Data as such data can no longer be used to identify a Data Subject.

6. Rights of Data Subjects

6.1. The Controller is primarily responsible for handling and responding to requests made by Data Subjects.

6.2. The Processor shall assist the Controller, especially through appropriate technical and organizational measures, insofar as this is possible, with the fulfillment of the Controller's obligation to comply with the rights of the Data Subjects and respond to Data Subjects' requests relating to their rights. In particular, the Service Provider shall assist as follows:

6.2.1. Correction, Blocking and Deletion. To the extent the Controller, in its use of the Services, cannot correct, amend, block or delete Personal Data, as required by Data Protection Legislation, Proxyclick shall comply with any request by the Controller to facilitate such actions to the extent Proxyclick is legally permitted to do

so. To the extent legally permitted, the Controller shall be responsible for any costs arising from Proxyclick's provision of such assistance.

6.2.2. Data Subject Requests. Taking into account the nature of the Processing, the Processor shall assists the Controller by appropriate technical and organizational measures, insofar as this is possible, for the fulfillment of the Controller's obligation to respond to requests for exercising the data subject's rights as set forth by applicable Data Protection Legislation (in particular Chapter III of the General Data Protection Regulation once it applies). Proxyclick shall provide the Controller with commercially reasonable cooperation and assistance in relation to the handling of a Data Subject's request for access to that Data Subject's own Personal Data, to the extent legally permitted and to the extent the Controller does not have access to such Personal Data through its use of the Services. If legally permitted, the Controller shall be responsible for any costs arising from Proxyclick's provision of such assistance.

6.2.3. Inquiry for information. Where, in accordance with applicable Data Protection Legislation, the Controller is obliged to answer a data subject's request for information related to the collection, processing or use of such data subject's data, Proxyclick shall support the Controller in providing the required information for all reasonable requests. The foregoing shall be applied only where the Controller has so instructed Proxyclick in writing. The Controller shall reimburse Proxyclick for the cost and expenses incurred in providing such support when the requests exceed the normal and reasonable amount.

7. Sub-processors

7.1. The Controller acknowledges and agrees that Proxyclick may engage third-party sub-processors in connection with the provision of the Services.

7.2. The current list of sub-processors forms the Appendix 2 to this DPA.

7.3. The Processor shall inform the Controller of any changes concerning the addition or replacement of sub-processors, thereby allowing the Controller to object to such changes. If the Controller has a reasonable basis to object to the Processor's use of a new Sub-processor, the Controller shall notify Proxyclick promptly in writing within ten (10) business days after receipt of Supplier's notice.

7.4. Where the Processor engages a sub-processor for carrying out specific Processing activities on behalf of the Controller, the same data protection obligations as set out in this DPA shall be imposed on that other processor by way of a contract or other legal act under Union or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the Processing will meet the requirements of applicable Data Protection Legislation. Where that other processor fails to fulfill its data protection obligations, Proxyclick shall remain liable for the acts and omissions of its Sub-processors.

8. Security

8.1. Within Processor's area of responsibility, Processor shall structure Processor's internal corporate organization to ensure compliance with the specific requirements of the protection of Personal Data under applicable Data Protection Legislation. Processor shall take the appropriate technical and organizational measures to adequately protect the Personal Data provided by Controller to Processor against misuse and loss in accordance with the requirements of Data Protection Legislation as set out in Annex 1.1. The technical and organizational measures form the appendix 1 to this DPA are

subject to technical progress and development, and Processor may implement adequate alternative measures. These must not however fall short of the level of security provided by the specified measures. Any material changes must be documented and Processor must provide Controller with the details upon request.

8.2. Using the Proxyclick platform as described in clause 5.7, Processor shall promptly notify Controller if it detects or reasonably suspects that a security incident has occurred which involves unauthorized disclosure, unauthorized access, misuse, loss, theft or accidental or unlawful destruction of Personal Data. Processor shall, in collaboration with the Controller, take adequate remedial measures as soon as possible. Furthermore, Processor shall promptly provide Controller with all relevant information as requested by Controller regarding such a data security incident. Processor shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken, and make such documentation available to the Controller at any time.

8.3. Decisions of the Processor which affect the security of its organization of the Processing of Personal Data, and the applied procedure shall be evaluated first in good faith with the Controller.

9. Data Storage and Transfer

9.1. The Personal Data collected from Data Subjects is processed inside the European Economic Area ("EEA"), or outside the EEA in accordance with clause 9.2.

9.2. To the extent Proxyclick uses sub-processors located outside the EEA, the Parties will cooperate in good faith in order to make sure that the necessary safeguards are implemented to make sure this processing outside the EEA complies with the Data Protection Legislation, which, except if agreed upon differently between the Parties, will consist of the Processor entering into standard contractual clauses with such sub-processor on behalf of the Controller. To that extent, the Controller awards the Processor the power of attorney to perform such actions on its behalf.

10. Term and Termination

10.1. This DPA begins upon the commencement of the Agreement and shall be in force and effect until the Agreement has been terminated or expires. If after the termination of the Agreement, further Processing of Personal Data by Processor is necessary for the winding-up of the Agreement or provided by law, e.g., regarding the return of Personal Data, this DPA shall continue to apply until the completion of the winding-up or return, as applicable.

10.2. The Parties agree that on the termination of the Agreement, the Processor shall, at the choice of Controller, return or delete all (copies of) the Personal Data processed on the Controller’s behalf, unless legislation imposed upon the Processor prevents it from returning or destroying all or part of the Personal Data transferred. To the extent Proxyclick would carry on any further processing of this personal data after termination of the Agreement and this DPA, it accepts that it is solely and fully responsible for these further processing activities.

11. Non-disclosure

11.1. The Processor shall not disclose any of the Personal Data or information received by the Processor in the course of the Agreement.

11.2. The Processor warrants that its employees, its subcontractors or any other person for which the Processor is responsible, and that is processing the Personal Data are suitably trained and shall keep the Personal Data confidential. The Processor will enter into non-disclosure agreements with its employees and subcontractors.

APPENDIX 1 TECHNICAL AND ORGANIZATIONAL MEASURES

1. Admittance controls

- Proxyclick offices are access-controlled with keys and are also protected by an alarm system
- Live customer data is only stored at AWS and OVH data centers which are certified and have strong physical security measures, e.g. barbed wire fences, video surveillance, motion detection systems, surveillance team on-site 24/7/365

2. Access controls to systems

- Interfaces to manage the infrastructure can be accessed only from a limited number of IP addresses
- Servers are protected with firewalls and an IDS (Intrusion Detection System)
- Access to the server is always granted via private key (not password) and IP addresses are blocked after a few failed attempts
- Access to the administration tool by support agents is protected by a password that contains at least 15 alphanumerical, mixed-case, randomly generated characters that is changed every month
- Laptops of Proxyclick staff are automatically locked after a period of inactivity of 5 minutes

3. Data access controls

- Proxyclick servers that store customer data cannot be reached directly from the public internet
- Proxyclick support staff is organized in three levels with separate permissions that are required for their level of support
- Access authorizations are granted to Proxyclick staff based on the Need-to-Know and Need-to-Do Principle corresponding to an authorization procedure (e.g. support staff may only access customer data when necessary to ensure account functionality)
- Audit trails for infrastructure changes are automatically generated

4. Distribution controls

- Customer data is stored on encrypted hard disks and is only electronically transferred
- Customer data sent over public networks is transmitted over HTTPS channels with authorization credentials
- Data that is transferred between servers managed by Proxyclick uses a private network.

5. Input controls

- Changes to data by users are logged in audit trails
- Audit trails contain the time of change, the user that performed the change and the content of the change

6. Order controls

- Hosting providers have no access to customer data
- Proxyclick audits the data center security measures
- Proxyclick carefully selects its third party data subprocessors and reviews them regularly. All such processors are contractually bound by Proxyclick to keep customer data confidential

7. Availability controls

- All customer data is backed up across multiple data centers and hosting providers
- High availability is guaranteed through duplication of the infrastructure in two geographically distant data centers and assured by hosting provider Service Level Agreements
- Failover procedures and documented and tested regularly
- Files uploaded by users on the application are virus scanned
- All servers are protected with firewalls
- Servers storing customer data are kept in private networks without direct inbound access over the internet
- An automatic monitoring system is in place to continuously check the state of the services and to send alerts to the appropriate personnel at Proxyclick.

8. Segregation controls

- Customers can define permissions at a very granular level. Permissions can be granted to groups of users
- Logical segmentation of customer data is enforced at code level
- Proxyclick data is separated from customer data
- The production, staging, testing and development environments are distinct

APPENDIX 2: CURRENT SUB-PROCESSORS

This appendix sets out the sub-processors processing Client Personal Data on behalf of Proxyclick.

Sub-processor (Company name, address)	Scope of processing	Types of personal data	Processing location	Applicable transfer mechanism (if applicable)
Proxyclick Inc, Avenue of the Americas 1177, New York, NY, 10036 USA	Support	All data	US	Standard Contractual Clauses
SendGrid Inc., 1801 California Street, Suite 500, Denver, Colorado 80202, USA	Email notifications	Name, email address	US	Standard Contractual Clauses
Twilio Inc., 375 Beale Street, Suite 300, San Francisco, CA 94105, USA	SMS notifications	Name, phone number	US	Standard Contractual Clauses
PubNub Inc., 725 Folsom Street San Francisco, CA 94107, USA	Data pushed into the apps	Visit ID Visitor ID	US	Standard Contractual Clauses
OVH SAS, 2 rue Kellermann BP 80157 59053 Roubaix Cedex 1, France	Hosting	All data (encrypted)	France	N/A
Amazon Web Services EMEA SARL, 38 avenue John F. Kennedy, 1855 Luxembourg	Hosting / backup	All data (encrypted)	Germany	N/A
Bugsnag Inc., 110 Sutter Street, Suite 1000, San Francisco, CA 94104, USA	Error and crash reporting (Dashboard)	Data linked to the error (can contain visitor data)	US	Standard Contractual Clauses
Raygun Ltd, L7, 59 Courtenay Place Te Aro, Wellington 6011, New Zealand	Error and crash reporting (iOS)	Data linked to the error (can contain visitor data)	NZ	Adequacy decision
[*Only if ID match feature is used*] Acuant Inc, 6080 Center Drive Suite 850 Los Angeles, CA 90045	ID scanning	ID card data	US	Standard Contractual Clauses
Microsoft Azure, Microsoft Ireland Operations Ltd, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P52	Face API, access control system and wifi & backup	Picture, everything in the backup	The Netherlands	N/A
[*Only if wifi integration is used*] Ironwifi LCC, 3071 N Orange Blossom Trail, Ste C, Orlando, FL 32804, USA	Wifi integration	Name or email address	US	Standard Contractual Clauses

Intercom R&D Unlimited Company, 2nd Floor, Stephen Court, 18-21 St. Stephen's Green, Dublin 2, Ireland	Support	All data	Ireland	N/A
HubSpot Ireland Limited, One Sir John Rogerson’s Quay, Dublin 2, Ireland	CRM	Name, email address, phone number and company name and details of users	Ireland	N/A
Support Your App Ltd., 1521 Concord Pike, Wilmington, DE 19803, USA	Support	All data	USA	Standard Contractual Clauses