DATA PROCESSING AGREEMENT

The Parties have entered into an agreement to establish the terms and conditions of the provision of visitor management and employee workflow services (the "Services") by Proxyclick to the Client (the "**Agreement**"). In the performance of this Agreement, Proxyclick, acting as the Processor, will be Processing Personal Data on behalf of the Client, acting as the Controller. This Data Processing Agreement ("**DPA**") details the conditions under which Proxyclick will perform these Processing activities.

All capitalized terms in this DPA will have the meaning as defined by the applicable privacy and data protection laws and regulations to the extent they apply to each Party and to the Processing of Personal Data under the Agreement, including the General Data Protection Regulation (EU) 2016/679 ("**GDPR**") (together, the "**Data Protection Legislation**"), unless the context requires otherwise.

If and insofar as the California Consumer Privacy Act of 2018 ("**CCPA**") applies to the Agreement, the definition in the Agreement (including this DPA) of: "Controller" includes "Business", "Processor" includes "Service Provider", "Data Subject" includes "Consumer" and "Personal Data" includes "Personal Information", in each case as defined under the CCPA**.**

Scope

The Client instructs Proxyclick to Process the following Personal Data for the purpose of the Agreement and pursuant to the DPA:

Data subject	Personal Data Categories
Employees of Client	First and last name
	Email address
	Phone number
	All other fields are optional and can be activated (or not) by the Client: e-mail address, phone, picture, signature, company name...
Visitors of Client	First and last name
	All other fields are optional and can be activated (or not) by the Client: e-mail address, phone, picture, signature, company name...

Provisions

1 RIGHTS AND OBLIGATIONS OF THE CLIENT

1.1 **Compliance.** The Client shall be solely responsible for complying with its obligations under the Data Protection Legislation, including, but not limited to, the lawfulness of the transmission to Proxyclick and the lawfulness of the Processing. The Client shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which the Client acquired Personal Data.

1.2 **Instructions.** The Client shall, in its use of the Service, only submit or otherwise have Personal Data Processed in accordance with the requirements of Data Protection Legislation. The Client instructs Proxyclick to Process Personal Data for the purpose of performing the Agreement and this DPA. The Client shall issue all additional Processing orders to Proxyclick in written form.

1.3 **Irregularities.** The Client shall inform Proxyclick without delay should it notice any mistakes or irregularities with respect to the Processing of Personal Data.

2 RIGHTS AND OBLIGATIONS OF PROXYCLICK

2.1 **Processing of Personal Data.** Proxyclick shall only Process Personal Data in accordance with the Agreement, the Data Protection Legislation and the written instructions of the Client, unless required to do so by legislation (including, but not limited to, Data Protection Legislation) to which Proxyclick is subject. In that case, Proxyclick shall inform the Client of that legal requirement before Processing, unless legally prohibited from doing so.

2.2 **Audit.** Proxyclick shall make available to the Client all information necessary to demonstrate compliance with the Data Protection Legislation, the Agreement, the DPA and the Client's instructions. Proxyclick shall allow for and contribute to audits, including inspections, conducted by the Client or another auditor mandated by the Client, provided that such auditor is subject to confidentiality obligations.

2.3 **Instruction in violation of Data Protection Legislation.** Proxyclick shall inform the Client if it concludes that an instruction of the Client may violate Data Protection Legislation. In this case, Proxyclick may interrupt the relevant Processing until instructions are confirmed or changed by the Client.

2.4 **Further use of aggregated data**. The Client authorizes Proxyclick to use Client Data that is aggregated and that does not reveal the Client's identity for the purpose of improvement of the Services and research and development. The aggregated data is no longer Personal Data as it can no longer be used to identify a Data Subject. Proxyclick accepts that it will be solely and fully responsible for these further activities.

2.5 **Assistance.**

2.5.1 Proxyclick will reasonably assist the Client, upon the Client's request, in ensuring compliance with the Client's obligations pursuant to Data Protection Legislation (in particular articles 32 to 36 of the GDPR, where applicable) taking into account the nature of Processing and the information available to Proxyclick.

2.5.2 Taking into account the nature of the Processing, Proxyclick will reasonably assist the Client by appropriate technical and organizational measures, insofar as this is possible, to comply with the rights of the Data Subjects as set forth by the Data Protection Legislation. If Proxyclick receives a request from a Data Subject, it shall transfer such request to the Client and act according to the Client's instructions. The Parties agree that Proxyclick can be in direct contact with the Data Subjects to provide technical support.

2.5.3 For all requests under Articles 2.5.1 and 2.5.2, Proxyclick shall assist insofar as it relates to Proxyclick's Processing of Personal Data under this DPA, to the extent the Client does not otherwise have access to the relevant information, and that such information is available to Proxyclick. To the extent legally permitted and insofar as the requests exceed the normal and reasonable amount, the Client shall be responsible for any costs arising from Proxyclick's provision of such assistance.

2.6 **Security**. Within Proxyclick's area of responsibility, Proxyclick shall structure its internal corporate organization to ensure compliance with the specific requirements of the protection of Personal Data under Data Protection Legislation.

2.6.1 Proxyclick shall take the appropriate technical and organizational measures to adequately protect the Personal Data provided by the Client against misuse and loss in accordance with the requirements of Data Protection Legislation.

2.6.2 Proxyclick's technical and organizational measures are set out in Annex 1 to this DPA. These are subject to technical progress and development, and Proxyclick may implement adequate alternative measures, which will not fall short of the level of security provided by the specified measures.

2.7 **Personal Data Breach**. Proxyclick shall promptly notify the Client if it detects or reasonably suspects that a Personal Data Breach has occurred, via the medium chosen by the Client on the Proxyclick platform (currently available at https://status.proxyclick.com). Proxyclick shall, in collaboration with the Client, take adequate remedial measures as soon as possible. Furthermore, Proxyclick shall promptly provide the Client with all relevant information as requested by the Client regarding the Personal Data Breach. Proxyclick shall document any Personal Data Breaches, comprising the facts relating to the Personal Data Breach, its effects and the remedial actions taken, and make such documentation available to the Client upon request.

2.8 **Confidentiality**. Article 8 of the Agreement shall apply in all its terms to Personal Data.

2.9 **CCPA.** Proxyclick shall not use, disclose, sell or retain the Personal Data for any purpose outside of this Agreement unless otherwise permitted by the applicable legislation (including Data Protection Legislation).

3 SUB-PROCESSORS

3.1 **Use of Sub-processors.** The Client acknowledges and agrees that Proxyclick may engage third-party sub-processors in connection with the provision of the Services.

3.2 **List of Sub-processors.** The current list of sub-processors forms the Annex 2 to this DPA. Proxyclick shall inform the Client of any changes concerning the addition or replacement of sub-processors, thereby allowing the Client to object to such changes. If the Client has a reasonable basis to object to Proxyclick's use of a new sub-processor, the Client shall notify Proxyclick promptly in writing within ten (10) business days after receipt of Proxyclick's notice.

3.3 **Sub-processors' Obligations.** Where Proxyclick engages a sub-processor for carrying out specific Processing activities on behalf of the Client, the same data protection obligations as set out in this DPA shall be imposed on that sub-processor by way of a contract, in particular providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the Processing will meet the requirements of Data Protection Legislation. Where the sub-processor fails to fulfil its data protection obligations, Proxyclick shall remain liable for the acts and omissions of its sub-processor.

4 DATA STORAGE AND TRANSFER

4.1 **Storage Location.** The Personal Data collected from Data Subjects is Processed inside the European Economic Area ("**EEA**"), or outside the EEA in accordance with Article 4.2.

4.2 **Data Transfers outside the EEA.**

4.2.1 To the extent Client is located outside the EEA in a country which is not subject to an adequacy decision under the GDPR, the EU Processor-to-Controller Standard Contractual Clauses ("**SCCs**") shall be incorporated by reference to this DPA. Annex 1 to the SCCs is deemed to be prepopulated with the names of Client, as data importer, and Proxyclick, as data exporter, and the Processing operations are deemed to be those described in the DPA. In case of conflict between the provisions of the SCCs and this DPA, the SCCs shall prevail.

4.2.2 To the extent Proxyclick uses sub-processors located outside the EEA, in a country which is not subject to an adequacy decision under the GDPR, such data transfer shall be subject to the Processor-to-Processor EU Standard Contractual Clauses.

5 TERM AND TERMINATION

5.1 **Term.** 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 Proxyclick 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.

5.2 **Termination.** The Parties agree that on the termination of the Agreement, Proxyclick shall, at the choice of Client, return or delete all (copies of) the Personal Data Processed on the Client's behalf, unless legislation imposed upon Proxyclick prevents it from returning or destroying all or part of the Personal Data transferred.

Schedule 1 to the DPA | Technical and Organizational Measures

1. Admittance controls

- Proxyclick offices are access controlled with keys and automated check-in procedure through the Proxyclick App, Proovr and a reception kiosk
- The offices are also protected by an alarm system
- Live customer data is only stored at Azure and OVH data centers which are certified (ISO27001, SOC1, SOC2...) 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
- Proxyclick staff are provided with a company-managed password manager to securely generate and manage their credentials
- Multi-Factor Authentication (MFA) is enforced for Proxyclick system administrators accessing core infrastructure

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 sub-processors and reviews them regularly. All such Processors are contractually bound by Proxyclick to keep customer data confidential and to process data according to applicable data protection laws.

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.

Schedule 2 to the DPA| List of current sub-processors

This Schedule sets out the sub-processors that Process Personal Data on behalf of Client.

Sub-processor Company Name	Sub-processor Address	Scope of Processing	Types of Personal Data	Processing location	Applicable transfer mechanism
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
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, All the data for backup (encrypted)	The Netherlands, Ireland	N/A
[*Only if wifi integration is used*] I**ronwifi 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 the data	Ireland	N/A
HubSpot Ireland Ltd.	One Sir John Rogerson's Quay, Dublin 2, Ireland	CRM	Name, email address, phone number, company name and details of users	Ireland, US	Standard Contractual Clauses
Support Your App Ltd.	1521 Concord Pike, Wilmington, DE 19803, USA	Support	All the data	US	Standard Contractual Clauses