Data Processing Agreement

Version: 2.8
Effective from: March, 23st, 2022

This Data Processing Agreement (DPA) forms an integral part of the arrangements between the Parties as agreed upon on _____ [DATE] (hereinafter referred to as: '**the Agreement**').

The Parties:

- _____ [NAME], having its registered office at _____ [STREET] in _____ [CITY], registered with the Chamber of Commerce under number _____ [COC NUMBER] and duly represented by Mr/Ms _____ [NAME] (hereinafter referred to as: '**the Controller**');
- **GoBright B.V**, having its registered office at **Van Hennaertweg 6** in **Alblasserdam**, registered with the Chamber of Commerce under number **67154808** and duly represented by **Mr. Hagoort** (hereinafter referred to as: '**the Processor**');

whereas:

- The Controller has entered into an agreement with its clients and the Controller wishes to engage the Processor in the performance of that agreement;
- The Controller and the Processor entered into an agreement (hereinafter referred to as: 'the Agreement') for the benefit of the above on _____ [DATE], for the purpose of **roommanagement (GoBright MEET) and deskmanagement (GoBright WORK), visitor management (GoBright VISIT) and digital signage (GoBright VIEW), and monitoring and analysis of data related to room, desk and visitormanagement and digital signage**;
- The Processor may be considered a Processor within the meaning of Article 4(8) of the General Data Protection Regulation (hereinafter referred to as: 'the GDPR') in the performance of the Agreement;
- The Controller is considered the Controller within the meaning of Article 4(7) of the GDPR;
- Reference made in this Data Processing Agreement to personal data refers to personal data within the meaning of Article 4(1) of the GDPR;
- The Controller will determine the purposes and means for the processing to which the conditions as set out in this agreement apply;
- The Processor is prepared to do so and is also prepared to comply with obligations relating to security and other aspects of the GDPR, insofar as this is within its power;
- The GDPR imposes on the Controller the obligation to ensure that the Processor provides sufficient guarantees in respect of the technical security measures and organisational measures governing the processing to be carried out;
- The GDPR additionally imposes on the Controller the obligation to ensure compliance with those measures;
- The Parties wish to lay down their rights and obligations in writing by means of this data processing agreement (hereinafter referred to as: 'the Data Processing Agreement'), partly in view of the requirements under Article 28(3) of the GDPR
- "SCC's" means the standard contractual clauses for processors as approved by the European Commission in decision 2021/914/EC for the transfer of personal data from processors in the EEA to processors established in third countries which do not ensure an adequate level of data protection, as described in Article 46 of the GDPR.

have agreed as follows:

Article 1. Purposes of the processing

1.1 The Processor undertakes to process personal data on the instruction of the Controller, subject to the conditions of this Data Processing Agreement. Processing will only take place within the framework of the Data Processing Agreement and for the purpose of offering the products and services of GoBright, and in order to achieve those objectives that have been laid down in the Agreement in mutual consultation.

1.2 The personal data that the Processor processes or will process within the framework of the Agreement and the categories of data subjects to whom the personal data pertain are set out in Appendix 1. The Processor will refrain from using the personal data for any purpose other than that determined by the Controller. The Controller will inform the Processor of the purposes of the processing insofar as these are not already stated in this Data Processing Agreement.

1.3 The Processor has no control of the purposes and the resources for the processing of personal data. The Processor will refrain from making any independent decisions with regard to the receipt and the use of the personal data, the provision thereof to third parties and the duration of storing personal data.

Article 2. Obligations of the Processor

2.1 With regard to the processing as referred to in Article 1, the Processor will ensure compliance with the conditions set by the GDPR with regard to the processing of personal data by the Processor based on its role.

2.2 The Processor will inform the Controller, at the latter's request and within a reasonable term, of the measures that it has taken in order to meet its obligations pursuant to this Data Processing Agreement.

2.3 The Processor's obligations arising from this Data Processing Agreement also apply to any party processing personal data under the authority of the Processor.

2.4 Under no circumstances will the processing of data by the Processor cause the Processor's databases to be expanded with data taken from the data sets provided by the Controller, unless it concerns the data in an aggregated, non-traceable form. In such case, the Processor is allowed to use these data for its own other purposes (e.g., improving the products and provided services).

2.5 The Processor will notify the Controller without delay if it feels that an instruction provided by the Controller violates the legislation referred to in paragraph 1.

Article 3. Transfer of personal data

3.1 The Processor may process the personal data in countries within the European Economic Area (hereinafter referred to as: 'the EEA'). Transfer to countries outside of the EEA is only permitted where it is done on the prior instruction/with the prior consent of the Controller, or where one of the adequate safeguards within the meaning of the GDPR is in place. Insofar Subprocessors as mentioned Appendix I might transfer personal data to those countries, these Subprocessors are bound to subject such transfers to the SCC's.

Article 4. Division of responsibility

4.1 The Processor will carry out the permitted processing activities within a computerised or semi-computerised environment.

4.2 The Processor is solely responsible for the processing of personal data under this Data Processing Agreement in accordance with the instructions of the Controller and under the express ultimate responsibility of the Controller. For any other processing of personal data, including but not limited to any collection of personal data by the Controller, processing for purposes not reported to the Processor, processing by third parties and/or for other purposes, the Processor does not accept any responsibility.

4.3 The Controller guarantees that the contents, the use and the instruction to process the personal data as referred to in the Data Processing Agreement are not unlawful and do not constitute a breach of any right of third parties.

Article 5. Engagement of third parties or Subprocessor

5.1 The Controller hereby gives the Processor its consent to engage a third party or Subprocessor in the processing of the personal data pursuant to this Agreement, with due observance of the applicable privacy legislation.

5.2 The Processor will inform the Controller of any intended changes concerning the addition or replacement of Subprocessors by sending Customer written notice thereof, if the Controller informed the Processor of a contact person to qs@gobright.com.
Such amendment will be deemed accepted and become effective 30 days after such notice unless Customer first gives Vendor written notice of objection to the intended change regarding the Subprocessors. If the Controller objects to Subprocessor engaged by the Processor, the Parties will consult in order to reach a solution.

5.3 In the rare event that the GoBright Platform or it's functionality is at acute risk of failure, degradation or outage, the Processor is allowed to make change in Subprocessors without first consulting, taken into account article 3 and 5.5, and sending notice without undue delay as intended in article 5.2 including its objection possibility.

5.4 The Processor at the time of conclusion of this Agreement only uses the Subprocessors listed in Appendix 1. The Controller gives the authorization of engaging these Subprocessors.

5.5 The Processor will in any case ensure that these third parties or Subprocessors assume the same obligations in writing as those agreed between the Controller and the Processor. The Processor warrants correct compliance with these obligations by such third parties and will, in the event of errors committed by such third parties, be liable towards the Controller for any loss suffered as if it had committed the errors itself.

Article 6. Security

6.1 The Processor takes appropriate technical and organisational measures against loss or any form of unlawful processing (such as unauthorised disclosure, interference, alteration or provision of personal data) in connection with the processing of personal data to be performed.

6.2 The Processor will make every effort to ensure that the security provided meets a standard that is not unreasonable in view of the state of the art, the sensitivity of the personal data and the costs associated with the security measures taken.

6.3 If a vital security measure is found to be absent, the Processor will ensure that the security provided meets a standard that is not unreasonable in view of the state of the art, the sensitivity of the personal data and the costs associated with the security measures taken.

Article 7. Duty to report

7.1 In the event of a data leak (which must be understood to denote a breach of the security, leading to the destruction, loss, alteration or unlawful provision of, or unlawful access to, data that have been forwarded, stored or otherwise processed, whether accidentally or unlawfully), the Processor will inform the Controller thereof without delay, or no later than within eighty-four (48) hours, on the basis of which information the Controller will decide whether or not it will inform the supervisory authorities and/or the data subjects. The Processor will make every effort to ensure that the information provided is complete, correct and accurate.

7.2 The Controller will ensure compliance with any statutory duties to report. Where necessary in order to comply with legal and/or regulatory requirements, the Processor will cooperate in informing the relevant authorities and, where appropriate, the data subjects.

7.3 The duty to report in any case involves reporting the fact that there has been a leak, as well as, insofar as known to the Processor:

- the date on which the leak occurred (or, if the exact date is not known, the period within which the leak occurred);
- the cause or suspected cause of the leak;
- the date and the time at which the Processor, or a third party or contractor engaged by the Processor, became aware of the leak;
- the number of people whose personal data have been breached (or, if the exact number is not known, the minimum and maximum number of people whose data have been breached);
- a description of the group of persons whose personal data have been breached, including a description of the type or types of personal data that have been breached;
- whether the data were encrypted, hashed or otherwise rendered incomprehensible or inaccessible to unauthorised parties;
- the measures that are intended to be taken and or have already been taken in order to close the leak and limit its consequences;
- contact details for following up on the report.

Article 8. Rights of data subjects

8.1 In the event that a data subject submits a request to exercise its statutory rights to the Processor, the Processor will forward the request to the Controller and inform the data subject thereof. The Controller will subsequently process the request independently. If the Controller requires the assistance of the Processor in handling a request from a data subject, the Processor may charge a fee in respect thereof.

Article 9. Duty of confidentiality

9.1 All personal data that the Processor receives from the Controller and/or collects itself within the framework of this Data Processing Agreement are subject to a duty of confidentiality towards third parties.

9.2 This duty of confidentiality does not apply insofar as the Controller has given explicit consent for providing the information to third parties, if providing the information to third parties is logically required in view of the nature of the instruction given and the performance of this Data Processing Agreement, or if there is a statutory obligation to provide the information to a third party.

Article 10. Audit

10.1 The Controller is authorised to have audits performed by an independent IT expert who is bound by a duty of confidentiality in order to verify compliance with all the aspects of this Data Processing Agreement.

10.2 This audit will only take place after the Controller has requested and assessed any similar audit reports that the Processor has available, and provides reasonable arguments that justify an audit initiated by the Controller after all. Such an audit is justified if any similar audit reports that the Processor has available provide an insufficient or inconclusive answer regarding the Processor's compliance with this Data Processing Agreement. The audit initiated by the Controller will take place two weeks after the Processor's prior notification, and no more than once a year.

10.3 As soon as possible and within a reasonable term, with a term of no more than two weeks being considered reasonable unless an urgent interest dictates otherwise, the Processor will cooperate in the audit, and it will make available any information and employees that may reasonably be relevant to the audit, including supporting information such as system logs. The Controller will ensure that the audit causes as little disruption to the other business operations of the Processor as possible.

10.4 The Parties will assess the findings of the audit that has been conducted in mutual consultation and determine on that basis whether or not those findings will be implemented

by one of the Parties or by both Parties jointly.

10.5 The reasonable costs of the audit will be borne by the Controller, on the understanding that the costs of the third party to be engaged will always be borne by the Controller.

10.6 The Processor will support the Controller in the performance of a Data Protection Impact Assessment (hereinafter referred to as: 'the DPIA') if the Processor is obliged to do so pursuant to the GDPR. As part of this support, among other things, the Processor will make the information required for the correct performance of the DPIA available to the Controller.

Article 11. Duration and termination

11.1 This Data Processing Agreement has been entered into for the term determined in the Agreement between the Parties, failing which it will in any case apply for the term of the collaboration.

11.2 The Data Processing Agreement cannot be terminated prematurely.

11.3 The Data Processing Agreement may be amended as set out in the GoBright License Subscription Agreement.

11.4 After termination of the Data Processing Agreement, the Processor will destroy the personal data received from the Controller without delay, unless the Parties agree otherwise.

Article 12. Other conditions

12.1 Liability clauses are strictly only arranged in the GoBright License Subscription Agreement.

12.2 The Data Processing Agreement and its execution are subject to Dutch law.

12.3 Any dispute that may arise between the Parties in connection with the Data Processing Agreement will be submitted to the competent court in the district of the court that is also competent to hear any dispute arising within the framework of the Agreement.

12.4 If one or more provisions of the Data Processing Agreement prove to be legally invalid, the other provisions of the Data Processing Agreement will remain in force. In such case, the Parties will consult on the invalid provisions in order to agree on a valid replacement provision, the purport of which is as close as possible to that of the provision that is to be replaced.

12.5 If the privacy laws change, the Parties will cooperate in amending this Data Processing Agreement in order to comply (or continue to comply) with this legislation.

12.6 Conflicts between different documents or annexes thereto, will be arranged as set out in the GoBright License Subscription Agreement

Thus agreed upon and signed,

Controller	**Processor**
_____/_____/_____	_____/_____/_____
Date	*Date*
_____	_____
Name	*Name*
_____	_____
Signature	*Signature*

Appendix 1: Specification of personal data and data subjects

Personal data
Within the framework of the Agreement, the Processor will process the following personal data on the Controller's instruction:

- User data (GoBright MEET, WORK, VISIT & VIEW):
    - Name
    - Email address
    - Phone number (optional)
    - Technical identifier of the user's NFC card (optional, if RFID/NFC is used)
- Booking details (GoBright MEET & WORK):
    - Date and time
    - Subject
    - Text of the booking (optional)
    - Organizer
    - Invitees
    - No-shows (booking, but not showing up) (optional)
- Visitors (GoBright VISIT):
    - Name
    - Email address (optional)
    - Phone number (optional)
    - Miniature picture (optional, only relevant for specific cases, determined by the Controller)
- IP-address

The Processor uses this data to perform and enable the purposes stated in the Agreement.

There is NO special personal data processed which relates to, or is similar to:
- Religion or belief
- Race
- Political preference
- Sexual life
- Trade union membership
- Criminal history
- Citizen service number

The Controller guarantees that the personal data and categories of data subjects as described in Appendix 1 are complete and correct, and indemnifies the Processor against any faults and claims that may result from an incorrect representation by the Controller.

Data retention
The data retention period is up to 1 year for historical data.
The datacenter level back-up is an overall systembackup with data stored 'cold' (not directly available) up to 5 months.

Technical and organizational measures
The Processor takes the necessary technical and organizational measures, as described in Article 6. These technical and organizational measures are safeguarded by means of the ISO 27001 based certified Information Security Management System that the Processor has implemented.

The implemented security measures include:
- ISO 27001 based certified Information Security Management System;
- Confidentiality agreements with GoBright employees and applicable contractors;
- Data storage encryption of personal data in the data storage on the platform;
- Transport encryption to external devices (such as the kiosk / room display / etc) via SSL or similar;
- Token-based authorization to the platform;
- Limited access to systems, servers and databases;
- Code and platform reviews of changes to the platform.

Access to personal data
Selected system administrators have access to the servers and databases for:
- the (further) development of the applications and the platform;
- posting a new version, build or update;
- the implementation of patches and hotfixes;
- making a backup.

Helpdesk employees, consultants and other employees of the Processor only have access to the customer data if this is necessary for the execution of the Agreement or if the customer has given permission for this.

Datacenters & hosting
The applications / platform of GoBright run on the Microsoft Azure platform.
The Microsoft Azure platform is, amongst others, SOC-2 & ISO 27001 certified and meets all national and international standards. The Microsoft data centers that Processor uses are located within the European Union.

Subprocessors

The following table lists the subprocessors used in delivering the GoBright platform:

Name **Place of business**	**Location of the processing**	**Type of service**	**Appropriate safeguards for transfers of personal information**
Microsoft Ireland Operations Limited Dublin, Ireland	The EEA (The Netherlands, Ireland)	Cloud platform service (Datacenter, Infrastructure)	EU law & SCC's Data encryption
Mailgun Technologies, Inc. San Antonio, USA Processed by subsidiary: Mailjet SAS Paris, France	The EEA (Germany, Belgium)	Transactional email	EU law & SCC's Data minimization
MessageBird B.V. Amsterdam, The Netherlands	The EEA (The Netherlands, Ireland)	Transactional SMS	EU law Data minimization
Google Ireland Limited Dublin, Ireland	The EEA (The Netherlands, Belgium)	Mobile push notifications (Firebase Cloud Messaging)	EU law & SCC's Data minimization