PRIVACY POLICY
regarding the Hotelify website and Hotelify application

Effective from 15th January 2024

The developer and operator of the Hotelify Application, Smart Hotel Solution Zrt. hereby informs the Users of the data management in the Hotelify Application and Hotelify Website (hotelify.net) as follows, in accordance with the Regulation (EU) 2016/679 of the European Parliament and of the Council on the General Data Protection Regulation (hereafter referred to as GDPR).

I. Data controller

Company name: Smart Hotel Solution Zrt.
Registered seat: 1118 Budapest, Szüret u. 15.
Company registration number: 01-10-141346
Tax number: 29249091-2-43
Email: info@hotelify.net;
Website: hotelify.net
Represented by: Endre Várszegi, CEO

II. Introduction

The Data Controller attaches great importance to the protection of personal data and continuously ensures the security of personal data. The Data Controller shall comply in all respects with the data protection provisions of the applicable legislation and the General Data Protection Regulation 2016/679 of the European Parliament and of the Council (GDPR).

Smart Hotel Solution Zrt. is entitled to modify the present Privacy Policy in any time. The present Privacy Policy is published on the Hotelify Website and is also available in the Hotelify Application. The present Privacy Policy takes into effect by publishing.

III. Data processing principals

1. *"Purpose limitation" principle*: personal data may only be processed for a specific purpose, for the exercise of a right or the performance of an obligation. The data must at all stages of processing be compatible with the purposes for which they are processed, and their collection and processing must be fair and lawful.

2. *"Lawfulness, fairness and transparency" principle*: Personal data must be processed lawfully and fairly and in a transparent manner for the data subject.

3. *"Proportionality, necessity or data minimisation" principle*: Only personal data that is necessary for the purpose for which it is processed and adequate for that purpose may be processed. The personal data may be processed only to the extent and for the duration necessary for the purpose. Accordingly, the Data Controller shall process only and exclusively such data as is strictly necessary for the purpose of the processing.

4. *"Accuracy" principle*: Data must be processed in such a way as to ensure that the data are accurate, complete and, where necessary for the purposes for which they are processed, kept up to date, and that the Data Subject can be identified only for the time necessary for the purposes for which they are processed.

5. *"Storage Limitation" principle*: Personal data must be kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be kept for longer periods only if the personal data will be processed for archiving purposes in the public interest, scientific and historical research purposes or statistical purposes in accordance with Article 89 (1) of Regulation EU 2016/679 (GDPR), subject to the implementation of appropriate technical and organisational measures required by the GDPR to protect the rights and freedoms of Data Subjects.

6. *"Integrity and Confidentiality" principle*: The Data Controller shall ensure the prevention of accidental or unlawful destruction or accidental loss, access, alteration or dissemination of personal data stored in automated data files by applying appropriate security measures to protect personal data.

7. *"Accountability" principle*: The Controller is responsible for compliance with the requirements set out in the paragraphs above and in this Privacy Policy and must be able to demonstrate such compliance.

8. *"Privacy by design" principle*: a very conscious approach to data protection, which in very brief terms means that the Data Controller implements appropriate technical and organisational measures, such as pseudonymisation, both in the definition of the way in which data are processed and in the course of processing, in order to effectively implement the above principles, fulfil obligations, incorporate legal safeguards, etc., and does so in a regulated and well-documented manner. In practice, the mindset is facilitated by training of Employees, data protection awareness, impact assessment, risk analysis, balancing of interests test used in the implementation and/or regular review of each data management.

9. The personal data shall retain this quality during the processing for as long as its relationship with the Data Subject can be re- established. The link with the Data Subject may be re-established if the Data Controller has the technical conditions necessary for such re-establishment.

IV. General provisions regarding data management activities

1. As a general rule, the processing of all data relating to the Data Subject in the context of the data processing activities and services performed by the Data Controller is based on free consent (Article 6 (1) point (a) GDPR), and its general purpose is to ensure the provision of the service and to maintain contact.

2. The above general rule is complemented by the processing required by law (Article 6 (1) point (c) GDPR), which the Data Controller informs the Data Subjects about when defining the individual processing.

3. As a general rule:

- for certain services, it is possible to provide additional information to help fully understand the Data Subject's needs, but this is not a condition for using the services provided by the Data Controller.
- personal data provided in the course of any processing activity are stored by the Data Controller in separate sets of data, separately from other data provided. These sets of data shall be accessible only to the Data Controller's authorised Employee(s).
- the Data Subject might request the modification, erasure and/or blocking of data recorded and stored in the course of any processing activity, as well as request detailed information on the processing, by sending a request to the e-mail address indicated in point I, unless otherwise specified in the definition of the processing activity.
- the provision of the data to be provided by the Data Subject in the course of each processing activity is a condition for the use of the services provided by the Data Controller.

4. Contact details of the natural person representatives of legal entity customers, buyers, suppliers:

The scope of personal data processed: name, address, telephone number, e-mail address, online identifier of the natural person.

Purpose of the processing of personal data: performance of a contract with a legal person partner of the Data Controller, business relationship, legal basis: consent of the Data Subject (Article 6 (1) point (a) GDPR).

Duration of storage of personal data: for 5 years from the business relationship or the Data Subject's capacity as a representative has been established.

V. Website visit data

1. No user data is recorded by the web server during the visit of the Website indicated in point I.

2. The Website of the Data Controller may also contain links to other sites that are not operated by the Data Controller, but are merely for the information of visitors. The Data Controller has no control over the content and security of the websites operated by partner companies and is therefore not responsible for them. It is the responsibility of the Data Subject to ensure that he/she is aware of the privacy policy of the sites he/she visits.

3. Some parts of the Website use so-called "cookies" - files that are stored on the hard drive of the Data Subject's hardware for the purpose of recording data and facilitating the identification and further visits of the Data Subject. The Data Subject can set his or her browser program to notify him or her when someone wishes to send a cookie and can choose whether to accept it. For more information about cookies, please visit http://www.cookiecentral.com.

The Data Controller uses the following cookies:

a.) Strictly necessary (essential) cookies: such cookies are essential for the proper functioning of the Website. Without the acceptance of these cookies, the Data Controller cannot guarantee that the Website shall function as expected, nor that all the information sought by the user will be available to the user. These cookies do not collect personal data from the Data Subject or data such can be used for marketing purposes.

b.) Functional cookies: these cookies ensure a consistent presentation of the Website tailored to the needs of the Data Subject and remember the settings chosen by the Data Subject.

c.) Targeted cookies: targeted cookies ensure that the advertisements displayed on the Website are tailored to the scope of interests of the Data Subject.

4. The Data Controller draws the attention of the users that cookies are automatically accepted by most internet browsers, but visitors have the option to delete them or to refuse them automatically.

5. On the Website, the Internet addresses of computers, IP addresses are logged to record the user's visit. By analysing these data, the Data Controller compiles statistics, for example, to determine how often users visit parts of the Website and how much time they spend there on occasion. IP addresses are not linked by the Data Controller to any other data by which the Data Subject could be personally identified and are used for statistical purposes only.

6. The Data Controller may display advertisements on the Website. The system collects personal data about the users who click on the advertisement. For more information on the scope of these data and how it is used, please refer to the Google Privacy Policy.

7. The Data Controller places a code set on the Website (or any subpage thereof), the purpose of which is to make the Data Controller's advertisement or advertisement available to users visiting the Website while they are browsing Google's websites and/or searching for the Data Controller or a term related to the Data Controller's services in Google's system. The code set does not collect, store or transmit any personal data. More information on the use and operation of the code set is available at http://support.google.com.

8. On the basis of the above, the Data Controller shall not use analytics systems to collect personal data.

9. The customer may visit the Website free of charge without providing any personal data. However, access to certain parts of the site is subject to registration, during which the customer provides information that constitutes personal data. By submitting and sending the data and by visiting the Website, the Customer consents to the processing of the provided data by the Data Controller in accordance with the law and this Privacy Policy, and consents to the processing of the data that may be considered as automated individual decisions as described below.

10. The Data Controller shall under no circumstances disclose personal data obtained during registration to any third party without the express consent of the Data Subject, except in cases of legal obligation or official proceedings, as well as to members of the company group and Data Processors.

11. The Data Controller excludes all liability for damages in case of destruction, delayed arrival or other defects of messages transmitted electronically. The Data Controller also excludes any liability for damages resulting from the downloading or unavailability of the Website.

12. Unless otherwise indicated, the content of the Website is the property of the Data Controller and is protected by copyright. The Data Controller reserves all rights in this respect.

VI. Data stored when filling out the contact form on hotelify.net (information request, customer database)

1. The Data Controller allows Data Subjects to request information from the Data Controller by providing the following details.

2. The request for information is based on free consent (Article 6 (1) point (a) GDPR).

3. The scope of Data Subjects: any natural person who contacts the Data Controller and requests information from the Data Controller, providing personal data.

4. Scope and purpose of the processed data:

name	identification
address	contact
phone number	contact
e-mail address	contact
message text	required to reply

5. The purpose of the processing is to contact the Data Subject and provide the Data Subject with appropriate information.

6. The activity and the process involved in the processing are the following: the Data Subject may consult the Data Controller about the Data Controller's services, products and/or other related matters through the means provided by the Data Controller and accessible to him/her. Data provided to the Data Controller via the Website are sent to the Data Controller by e- mail. The Data Controller, through the Employee in charge of this task, shall answer the Data Subject's question and shall send it to the Data Subject in the same way as the request for information was received, unless the Data Subject has provided otherwise. The Data Subject, in accordance with the purpose of the processing, freely consents to being contacted by the Data Controller, through the contact details provided by him/her in the request for information, in order to clarify or answer the question.

7. Duration of data processing: until the purpose is achieved. 2 years after the end of the bidding period.

VII. Data stored during the creation of a user profile in the Hotelify application

Subject	Data category	Data origin	Purpose of data management	Legal basis of data management	Duration of data management
User registered within Hotelify	Name*	from Subject	User identification, communication	GDPR Article 6. (1) b,	the data shall be stored for 5 years after the termination of the registration (general term of statute of limitation)
User registered within Hotelify	E-mail address*	from Subject	User identification, communication	GDPR Article 6. (1) b,	the data shall be stored for 5 years after the termination of the registration (general term of statute of limitation)
User registered within Hotelify	Phone number	from Subject	User identification, communication	GDPR Article 6. (1) b,	the data shall be stored for 5 years after the termination of the registration (general term of statute of limitation)
User registered within Hotelify	Address	from Subject	User identification, communication	GDPR Article 6. (1) b,	the data shall be stored for 5 years after the termination of the registration (general term of statute of limitation)
User registered within Hotelify	Password	from Subject	User identification, communication	GDPR Article 6. (1) b,	the data shall be stored for 5 years after the termination of the registration (general term of statute of limitation)

Data marked with * are mandatory to fill in, without these data Hotelify account registration is not possible.

VIII. Complaint handling

1. The Data Controller shall provide the opportunity for the Data Subject to make a complaint orally (in person, by telephone) or in writing (e-mail, post) regarding the conduct, activity or omission of the Data Controller.

2. The scope of Data Subjects: any natural person who wishes to lodge a complaint against the Data Controller.

3. The purpose of data processing: to identify the Data Subject and the complaint, and to record data required by law.

4. Scope and purpose of the processed data:

name	identification
identifier of the complaint	identification
date of receipt of the complaint	identification
phone number	contact
personal data provided during the conversation	identification
billing/mailing address	contact
the complaint	investigation of the complaint

5. The purpose of the data processing is to ensure that the complaint is made and to maintain contact.

6. The activity and process involved in the data processing:

- The Data Subject shall communicate his/her complaint to the Data Controller orally or in writing.
- If the Data Subject makes a complaint orally, the Data Controller will take a minute of the complaint.
- The Data Controller will investigate and respond to the complaint within a reasonable time.

7. Duration of data processing: the Data Controller shall keep the minute of the complaint and a copy of the response for three years pursuant to paragraph (7) of Article 17/A of Act CLV of 1997 on Consumer Protection.

IX. Rights of Data Subjects

1. The Data Controller informs the Data Subjects that they can exercise their rights in person or by sending a request to the e-mail or postal address of the Data Controller, or by requesting information from these contact details.

2. The Data Controller shall examine and respond to the request as soon as possible after receipt, but within a maximum of 25 days, and will take the necessary steps in accordance with the provisions of this policy, the internal rules and the law.

3. Right to information, also known as the data subject's "right of access"
The Data Controller shall provide information at the request of the Data Subject:

- the data and categories of personal data it processes,
- the purpose, the legal basis and duration of the data processing,
- the duration of storage of the data or, where this is not possible, the criteria for determining that duration,
- if the data have not been collected from the Data Subject, information about their source,
- the data of Data Processor, if the Data Controller has engaged a Data Processor,
- the circumstances of the personal data breach, its effects and the measures taken to remedy it, and
- if the personal data of the Data Subject are transferred, the legal basis, purpose and recipient of the transfer.

4. The information is free of charge if the person requesting the information has not yet submitted a request for information to the Data Controller for the same set of data in the current year. In other cases, a fee may be charged. The fee already paid shall be refunded if the data have been unlawfully processed or if the request for information has led to a rectification.

5. The Data Controller shall refuse to provide information if, pursuant to a law, an international treaty or a provision of a binding legal act of the European Union, the Data Controller receives personal data in such a way that the controller who transfers the data notifies the Data Subject of the restriction of his or her rights under the said law or other restriction of the processing of the personal data, the external and internal security of the State, such as national defence, national security, the prevention or prosecution of criminal offences, the security of law enforcement, the economic or financial interests of the State or local authorities, the important economic or financial interests of the European Union, the prevention and detection of disciplinary or ethical offences in connection with the exercise of the profession, infringements of labour law or the protection of the rights of the Data Subject or of others, including in all cases for the purposes of control and supervision.

6. The Data Controller shall notify the Hungarian National Authority for Data Protection and Freedom of Information of rejected requests for information annually by 31 January of the year following the year in question.

7. Right of rectification: the Data Subject has the right to obtain, upon request, the rectification of inaccurate personal data relating to him or her by the Data Controller without undue delay. Having regard to the purposes of the processing, the Data Subject shall have the right to request the completion of incomplete personal data, including by means of a supplementary declaration. If the personal data is inaccurate and the accurate personal data is available to the Data Controller, the Data Controller shall rectify the personal data without the Data Subject's request.

8. The right to erasure, also known as the "right to be forgotten": the Data Subject has the right to obtain from the Data Controller, upon his or her request, the erasure of personal data relating to him or her without undue delay, and the Data Controller is obliged to erase personal data relating to the Data Subject without undue delay, unless it is precluded by mandatory data management. In addition to the above, the Data Controller shall delete the data if:

- the data processing is unlawful;
- the data are incomplete or inaccurate - and this situation cannot be lawfully remedied - provided that erasure is not excluded by law;
- the purpose of the processing has ceased or the statutory time limit for storing the data has expired or ordered by a court or the Authority;
- the personal data are no longer necessary for the purposes for which they were collected or otherwise processed;
- the Data Subject objects to the processing and there are no overriding legitimate grounds for the processing;
- the personal data were collected in connection with the provision of information society services directly to children as referred to in Article 8 (1) of the GDPR.

9. In the event that the Data Controller has disclosed the personal data for any reason and is required to delete it pursuant to the above, it shall take reasonable steps, including technical measures, taking into account the available technology and the cost of implementation, to inform other controllers that have processed the data that the Data Subject has requested the deletion of the links to or copies or replicas of the personal data in question.

10. The Data Controller draws the attention of the Data Subjects to the limitations of the right to erasure or "right to be forgotten" under the GDPR, which are:

- exercise the right to freedom of expression and information;
- to comply with an obligation under Union or Member State law that requires the Data Controller to process personal data or to carry out a task carried out in the public interest or in the exercise of official authority vested in the Data Controller;
- public interest in the field of public health;
- for archiving purposes in the public interest, scientific and historical research purposes or statistical purposes in accordance with Article 89 (1) of the GDPR, where the right to erasure would be likely to render impossible or seriously impair such processing; or
- bringing, asserting or defending legal claims.

11. Right to restriction of processing, right to blocking
The Data Subject has the right to have the Data Controller restrict processing at his/her request. If, on the basis of the information available to him/her, it can be assumed that erasure would harm the legitimate interests of the Data Subject, the data shall be blocked. Personal data blocked in this way may be processed only for as long as the processing purpose which precluded the deletion of the personal data continues to exist. Where the Data Subject contests the accuracy or correctness of the personal data, but the inaccuracy or incorrectness of the contested personal data cannot be clearly established, the data shall be blocked. In this case, the restriction shall apply for the period of time necessary to allow the Data Controller to verify the accuracy of the personal data. The data shall be blocked if the processing is unlawful and the Data Subject opposes the erasure of the data and requests instead the restriction of their use, or the Data Controller no longer needs the personal data for the purposes of the processing but the Data Subject requires them for the establishment, exercise or defence of legal claims or the Data Subject has objected to the processing; in which case the restriction shall apply for the period until it is established whether the legitimate grounds of the Data Controller prevail over the legitimate grounds of the Data Subject. Where processing is subject to restriction (blocking), such personal data may be processed, except for storage, only with the consent of the Data Subject or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for important public interests of the Union or of a Member State.

12. The Data Controller draws the attention of the Data Subjects to the fact that the right of the Data Subject to rectification, erasure or blocking may be restricted by law in the interests of the external and internal security of the State, such as national defence, national security, the prevention or prosecution of criminal offences, the security of law enforcement, or for reasons of economic or financial interest of the State or local government, important economic or financial interests of the European Union, for the purpose of the prevention and investigation of disciplinary or ethical offences and of breaches of labour law or employment protection rules, including in all cases for the purposes of control and supervision, and for the protection of the rights of the Data Subject or of others.

13. The Data Controller shall, without undue delay and within a maximum of 25 days of receipt of the request, inform the Data Subject of the data subject of the request and/or rectify the data and/or erase and/or block the data or take other steps in accordance with the request, unless there are grounds for exclusion.

14. The Data Controller shall notify the Data Subject in writing of the rectification, erasure or restriction of processing, as well as all those to whom the data were previously transmitted or transferred for processing. The Data Controller shall inform the Data Subject, at his or her request, of the identity of those recipients. Notification may be dispensed with where this would not be contrary to the legitimate interests of the Data Subject, having regard to the purposes of the processing, or where the provision of the information proves impossible or would involve a disproportionate effort. The controller shall also notify the Data Subject in writing if the exercise of the Data Subject's rights cannot be exercised for any reason and shall specify the factual and legal grounds and the remedies available to the Data Subject: appeal to the court and the Hungarian National Authority for Data Protection and Freedom of Information.

15. The "right to data portability"
The Data Subject has the right to receive the personal data concerning him or her which he or she has provided to the Data Controller in a structured, commonly used, machine-readable format and the right to transmit these data to another controller without hindrance from the Data Controller to which he or she has provided the personal data, if the processing is based on consent; and the processing is automated. In exercising the right to data portability, the Data Subject shall have the right to request, where technically feasible, the direct transfer of personal data between controllers. The exercise of this right shall be without prejudice to the right to erasure. This right shall not apply where the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Data Controller. The exercise of this right shall not adversely affect the rights and freedoms of others.

16. Right to object
The Data Subject may object to the processing of his or her personal data, including profiling, if

- the processing (transfer) of personal data is necessary solely for the purposes of the exercise of a right or legitimate interest pursued by the Data Controller or the recipient, except in cases of mandatory processing;
- the personal data are used or disclosed for direct marketing, public opinion polling or scientific research purposes;
- the exercise of the right to object is otherwise permitted by law.

The Data Subject may also object to the processing of personal data for direct marketing purposes on the basis of Article 21(3) of the GDPR, in which case the personal data shall no longer be processed for such purposes. Where personal data are processed for scientific or historical research purposes or statistical purposes, the Data Subject shall have the right to object to the processing of personal data concerning him or her on grounds relating to his or her particular situation, unless the processing is necessary for the performance of a task carried out for reasons of public interest.

17. The Data Controller shall examine the objection within the shortest possible period of time from the date of the request, but not later than 25 days, and shall inform the applicant in writing of the outcome of the examination, with the simultaneous suspension of the processing. If the applicant's objection is justified, the Data Controller shall terminate the processing, including any further collection and transmission, and block the data, and notify the objection and the action taken on the basis of the objection to all those to whom the personal data concerned by the objection have been previously disclosed and who are obliged to take measures to enforce the right to object.

18. If the Data Subject shall not agree with the decision of the Data Controller or if the Data Controller fails to comply with the time limit, the data subject has the right to appeal to the court within 30 days of the decision being notified.

19. Rights of the Data Subject in relation to automated decision-making, including profiling: a decision based on an assessment of the personal data of the Data Subject may be taken solely by automated processing only if it is made in the course of entering into, or performance of, a contract, provided that it is initiated by the Data Subject or is permitted by a law which also lays down measures to safeguard the Data Subject's legitimate interests.
In the case of a decision taken by automated processing, the Data Subject shall, upon request, be informed of the method used and its essence and shall be given the opportunity to express his or her point of view.

20. Enforcement in court
The Data Subject may take legal action (appeal to the court) in case of a breach of his or her rights. The
court is acting out of turn in the case. The Data Controller is obliged to prove that the processing is in compliance with the law.

21. In the event of a violation of his/her right to information self-determination, the Data Subject may lodge a complaint to: Hungarian National Authority for Data Protection and Freedom of Information (1055 Budapest, Falk Miksa utca 9-11.; postal address: 1363 Budapest, Pf. 9; /telephone: +36 (1) 391-1400; e-mail: ugyfelszolgalat@naih.hu; website: www.naih.hu).

22. A complaint or a complaint in case of violation of rights in relation to content that is offensive to minors, hateful, exclusionary, corrective, violation of the rights of a deceased person, violation of reputation shall be filed to: Hungarian National Media and Infocommunications Authority (1015 Budapest, Ostrom u. 23-25.; postal address: 1525. Pf. 75; telephone: (06 1) 457 7100; e-mail: info@nmhh.hu).

23. Legal rules on compensation and damages: in the event that the Data Controller infringes the Data Subject's right to privacy by unlawfully processing the Data Subject's data or by breaching the requirements of data security, the Data Subject may claim damages from the Data Controller.

In the event that the Data Controller has engaged a Data Processor, the Data Controller shall be liable to the Data Subject for any damage caused by the Data Processor and the Data Controller shall also pay to the Data Subject the damages for any personal injury caused by the Data Processor. The Data Controller shall be exempted from liability for the damage caused and from the obligation to pay the damage fee if it proves that the damage or the infringement of the Data Subject's right to privacy was caused by an unavoidable cause outside the scope of the processing.

No compensation shall be due and no damages shall be payable in so far as the damage or injury to the person concerned has been caused by the intentional or grossly negligent conduct of the Data Subject.

X. Data security

1. The Data Controller shall ensure the security of the data. To this end, it shall take the necessary technical and organisational measures with regard to the data files stored by means of IT tools.

2. The Data Controller shall ensure that the data security rules provided for in the applicable legislation are complied with.

3. The Data Controller shall ensure the security of the data, take the technical and organisational measures and establish the procedural rules necessary to enforce the applicable laws, data protection and confidentiality rules.

4. The Data Controller shall take appropriate measures to protect the data against unauthorised access, alteration, transfer, disclosure, deletion or destruction, accidental destruction or damage and against inaccessibility resulting from changes in the technology used.

5. When determining and applying measures to ensure the security of the data, the Data Controller shall take into account the state of the art and shall choose among several possible processing solutions the one which ensures a higher level of protection of personal data, unless this would involve a disproportionate effort.

6. The Data Controller applies the following security measures:
(i) only persons expressly authorised and bound by confidentiality obligations may have access to the data;
(ii) the computers and mobile devices (other data carriers) used in the processing are owned by the Data Controller;
(iii) the computer system containing personal data used by the Data Controller is equipped with virus protection;
(iv) the use of backups and archiving to ensure the security of digitally stored data;
(v) access to the data on the computers and to the administrative interface only with a user name and encrypted password;
(vi) ensuring the continued confidentiality, integrity, availability and resilience of the systems and services used to process personal data;
(vii) access to and availability of personal data can be restored in a timely manner in the event of a physical or technical incident;
(viii) to store the processed data in a manner that prevents unauthorised access.
(ix) the removal of personal data from paper data carriers by means of shredding or by using an external organisation specialised in shredding; in the case of electronic data carriers, the physical destruction of the data in accordance with the rules on the disposal of electronic data carriers, if necessary, with prior secure and irretrievable deletion of the data;

This Privacy Policy is governed by Hungarian law. This Privacy Policy is available in English and Hungarian. In case of any discrepancy, the Hungarian version shall prevail.

15. 01. 2024.
Smart Hotel Solution Zrt.