Data Sharing Addendum (Hotel) - Version: 10/10/23

In addition to the privacy terms as set out in the Agreement, the following terms apply to the processing of Personal Data provided to the Hotel in accordance with the Agreement.

This Data Sharing Addendum (the "**Addendum**"), is effective as of the date both Parties execute the agreement, constitutes an integral part of all agreements (the "**Agreement(s)**" between an entity of the EFG Group for and on behalf of itself, its Affiliates and/or their respective subsidiaries (collectively "**EFG**") and the Hotel for and on behalf of itself and its Affiliates each a "**Party**", together the "**Parties**".

1. DEFINITIONS

1.1 "**Applicable Data Protection Laws**" means: the EU General Data Protection Regulation 2016/679 ("**GDPR**"), the European Privacy and Electronic Communications Directive (Directive 2002/58/EC) and any laws of Member States of the European Economic Area ("EEA") that implement or supplement the GDPR and/or the Directive, the UK GDPR, the UK Data Protection Act 2018 and the UK Privacy and Electronic Communications Regulations 2003, and all other applicable laws and regulations relating to the processing of personal data and privacy.

1.2 "**Controller**" shall have the meaning given to it in GDPR;

1.3 "**Permitted Purpose**" means the purposes as described in the Agreement (or as otherwise agreed in writing by the parties);

1.4 **"EU SCCs"** means the contractual clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council ("**EU SCCs**"), Module One (Controller to Controller);

1.5 "**UK SCCs**" means standard data protection clauses adopted pursuant to Article 46(2)(c) or (d) of the UK GDPR (specifically, the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses)

2. GENERAL PROVISIONS

2.1 Parties agree that EFG and Hotel are separate independent controllers for the Processing of Personal Data. Each party shall be individually and separately responsible for complying with the obligations that apply to it as a Controller under Applicable Data Protection Laws.

2.2 EFG shares Personal Data with the Hotel for the purpose of obtaining the Services from the Hotel as set out in the Agreement. Hotel will at all times only Process Personal Data for the purposes of providing the Services to EFG, as set out in the Agreement.

2.3 The Hotel shall not sell or market Personal Data.

2.4 The Hotel shall and shall ensure that any EFG Personal Data received as part of the Services, will only be processed for the Permitted Purpose as described in the Agreement.

3. PERSONAL DATA BREACHES

3.1 The Hotel cooperates and assists EFG with the fulfillment of EFG's data breach reporting obligations.

3.2 Upon becoming aware of a Personal Data Breach, Hotel shall without undue delay, but ultimately within 72 hours of becoming aware of such Personal Data Breach, inform EFG and provide written details of the Personal Data Breach, including but not limited to a the nature and the cause of the breach, the (approximate) number of Data Subjects concerned, the categories and approximate number of personal data records concerned, and the measures taken or proposed to be taken to address it.

3.3 The Hotel shall take measures and actions as are appropriate to remedy or mitigate the effects of the Personal Data Breach.

4. ASSISTANCE

4.1 The Hotel shall provide reasonable and timely assistance to EFG, to enable EFG to respond to: (i) any legitimate request from an individual to exercise any of its rights under Applicable Data Protection Laws (including its rights of access, correction, objection, erasure and data portability, as applicable); and (ii) any other correspondence, enquiry or complaint received from a regulator or court or any third party in connection with the processing of the Personal Data.

5. INTERNATIONAL DATA TRANSFERS

5.1 For the transfer of Personal Data relating to individuals in the European Economic Area ("EEA") or the UK by EFG as data exporter to the Hotel located in a country outside the EEA or the UK not declared as providing adequate level of data protection by the European Commission (Article 45(3) GDPR), Parties agree to enter into Standard Contractual Clauses, which are incorporated by reference and form part of this ADDENDUM as follows:

5.2 In relation to Personal Data about individuals in the EEA, the EU SCCs will apply completed as follows:

A. Module One of the EU SCCs applies

B. Clause 7, the optional docking clause, applies;

C. Clause 17, option 1 applies, and the EU SCCs will be governed by the laws of the State Commissioner for Data Protection and Freedom of Information North Rhine-Westphalia;

D. in Clause 18(b), disputes shall be resolved before the courts of North Rhine-Westphalia , Germany

E. Annex I of the EU SCCs shall be deemed completed with the information set out in Schedule 1 to this ADDENDUM ; and

F. Annex II of the EU SCCs shall be deemed completed with the information set out in Schedule 2 to this ADDENDUM .

5.3 In relation to Personal Data relating to individuals in the UK, the UK SCCs will apply completed as follows:

A. The EU SCCs, completed as set out above in clause 5.2 of this ADDENDUM shall apply to transfers of such Personal Data, subject to sub-clause (b) below; and

B. The UK Addendum shall be deemed executed between EFG and the Hotel and the EU SCCs shall be deemed amended as specified by the UK Addendum in respect of the transfer of such Personal Data.

6. GENERAL

6.1 This Agreement shall survive so long as Hotel Processes Personal Data. Upon EFG's request, or upon termination or expiry of this Agreement.

6.2 In the event of any conflict or inconsistency between any of the provision of this Addendum, the Agreement(s), or the Standard Contractual Clauses (if applicable), the terms or conditions of the Standard Contractual Clauses (if applicable) shall control, then this Addendum, then the Agreement.

6.3 This Agreement may not be modified except by a subsequent written instrument signed by both Parties.

6.4 The Hotel shall indemnify EFG from and against all loss, cost, harm, expense (including reasonable legal fees), liabilities or damage suffered or incurred by EFG as a result of the Hotel's breach of Applicable Data Protection Laws, and as a result of a Personal Data Breach that occurred at the Hotel.

6.5 If any part of this Agreement is held unenforceable, the validity of all remaining parts will not be affected.

Schedule 1
Data Transfer Description (Annex I, EU SCCs)

A. LIST OF PARTIES

Controller(s) / Data exporter(s):

1.	Name:	As set out in the Agreement
	Address:	As set out in the Agreement
	Contact person's name, position and contact details:	Darryl Anthony, VP Data & Privacy, privacy@efg.gg
	Activities relevant to the data transferred under these Clauses:	The activities specified under Annex I(B) below.
	Signature and date:	This Annex I shall automatically be deemed executed when the Addendum is executed by EFG.
	Role (controller/processor):	Controller

Controller(s)) / Data importer(s):

1.	Name:	The entity identified as the Hotel in the Agreement
	Address:	The Hotel's address as set out in the Agreement
	Contact person's name, position and contact details:	The contact details set out in the Agreement
	Activities relevant to the data transferred under these Clauses:	The activities specified under Annex I(B) below.
	Signature and date:	This Annex I shall automatically be deemed executed when the Agreement is executed by the Hotel.
	Role (controller/processor):	Controller

B. DESCRIPTION OF THE TRANSFER

EU SCC Module:	C2C (Module 1)
Categories of Data Subjects:	Where applicable: ● EFG personnel/staff ● EFG guests / attendees
Purpose(s) of the data transfer and further processing/ processing operations:	The provision of the Services to EFG as set out in the Agreement
Categories of Personal Data:	Booking information including, but not limited to, name, home address, telephone number, email address, nationality, check-in information, passport details, food preferences.
Sensitive data transferred (if applicable) and applied restrictions or safeguards:	● Passport Information that contains Biometric data ● Any physical attributes or allergies shared (e.g., disabilities, nut allergy)

EU SCC Module:	C2C (Module 1)
Frequency of the transfer:	As required for the event dates as set out in the Agreement
Nature and subject matter of the processing:	Collection, usage, storage and deletion of personal data for the provision of the services to EFG as set out in the Agreement.
Duration of the processing:	The duration of the transfer under this Addendum is until the termination of the Agreement in accordance with its terms plus the period from the expiry of the Agreement until deletion of the Personal Data by Vendor in accordance with the terms of the Agreement.
Retention period (or, if not possible to determine, the criterial used to determine the period):	90 Days post expiration/termination of the Agreement or as set out in the Agreement

C. COMPETENT SUPERVISORY AUTHORITY

Competent supervisory authority/ies in accordance (e.g., in accordance with Clause 13 SCCs):	When the EU GDPR applies, the competent supervisory authority shall be, the State Commissioner for Data Protection and Freedom of Information North Rhine-Westphalia, Kavalleriestr. 2-4, 40213 Düsseldorf When the UK GDPR applies, the competent supervisory authority shall be the UK Information Commissioner's Office.

Schedule 2: Security Measures
(Annex II, EU SCCs)

Description of the technical and organisational measures implemented by the Data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons:

A. Organisational Control

Measures, which comply with the specific requests of Data Protection, regarding the internal organisation:

- Instalment of an external Data Protection Officer with expertise
- Commitment of employees to data secrecy
- IT-Emergency concept
- Data back-up concept (for production data)
- Regulations regarding the correct and secure processing of duties done by data processing
- Regular instruction of relevant regulations
- Control of compliance with the regulations
- Organisational, spatial and/or personal separation of data processing from other business units and other customers
- Regulations and instructions for entry control
- Regulations and instructions for admission control
- Regulations and instructions for access control
- Regulations and instructions for transport of data storage media and transmission control
- Regular information and instruction of the employees
- Regulations and instructions for dealing with requests from Data Subjects for exercise of Data Subject rights including access, deletion and portability
- Description of activities in working instructions
- Data deletion concept
- External Certifications or internal data privacy audit
- Documentation of IT-procedures, software, IT-configuration
- Regular, periodic reviews of regulations and instructions

B. Entry Control

Measures to limit entrance of unauthorized persons to areas where personal data is used or processed with electronic data processing devices.

- Entry control
- Regulations and instructions of entry control
- Gate control
- Identification badges / code cards
- Entry regulations organisation for employees
- Entry regulations for external service providers (cleaning and maintenance personal, craftsmen, customers, visitors
- Classification of security areas
- Identification of admission authorized persons
- Safeguarding by alarm system, intrusion detector, police emergency call
- Security locks with centralized key administration and master key plan
- Revision secure organisation of admission rights
- Revision secure grant and revocation of admission rights

C. Admission Control

Measures to limit admission of unauthorized persons to systems where personal data is used or processed with electronic data processing devices.

- Safeguarding of physical network infrastructure
- Firewall for internal networks against external vulnerabilities
- Mechanisms for intrusion detection and notification of security events
- Control of use for electronic data processing
- Regulations and instructions of admission control
- Control and identification of authorized persons
- Logging of use for entry rights and regular reports
- Admission only with User-ID and password only
- Separation of function principle when granting entry authorisation
- Identification of terminal or terminal user (e.g.: login with user-ID and password)
- Limitation of false log-in attempts
- Automatic screensaver protection in case of inactivity
- Lockable terminals and decentralised IT-systems

- Safeguarding of electronic data processing systems correspondent with the requirements
- Functional and/or timely limited use of terminals

D. Access Control (Electronic data processing)

Measures to limit access of unauthorized persons to systems where personal data is used or processed with electronic data processing devices.

- Regulations and instructions for access control
- Processes for file organisation
- Rights- and role-concept
- Assignment of rights for data-input as well as for information, modification and deletion of stored data
- Regulated procedure for granting, changing and revocation of access rights
- Selective access regulations for procedures, operation control tickets
- User adaptive access protection
- Selective access for files and functions
- Automatic screensaver protection in case of inactivity
- Requirement of user identifiers (Passwords) for files, system data, application data
- Machine control of authorisations
- Logging access to specific data (e.g.: Console log, machine Log)
- Functional and/or timely limited use of terminals
- Password policy at the level of configuration of IT-systems
- Identification and authentication of users
- Control of administrator activities
- Specific written directives for the restart-procedure
- Safeguards for access by self-acting institutions
- Use of encryption for the protection of data during transmission and during storage.

E. Access Control (Data media)

Measures to limit access of unauthorized persons to data and/or applications being stored on storage devices outside of an electronic data processing system.

- Write-protection for data media
- Identification of authorized personnel
- Rules regarding the production of copies
- Labelling obligation for data media with classification
- Guidelines for the organisation of data storage
- Controlled storage of in use and swapped out data media in a secure area (Archive, secure cabinets)
- Definitions of areas which are suitable or scheduled for the storage of data media (e.g.: disc, volume, tape, cartridge)

F. Transmission Control

Measures to ensure that personal data cannot be read, copied, modified or removed without authorisation during electronic transmission or transport.

Measures to ensure and that it is possible to check and establish to which bodies the transfer of personal data by means of data transmission facilities is envisaged.

Measures to ensure, that an automated procedure for the retrieval of personal data is running a log procedure in order to have retrospect information which data has been retrieved by whom.

- Determination of authorized person for transmission and transport
- Documentation of the retrieval and transmission programs
- Determination and documentation of the transmission procedure and the data receivers
- Protocol of data transmission and receivers
- Regulations and instructions for data media transport and transmission control
- Secured data lines
- Use of cryptographic procedures as far as useful or mandatory
- Electronic signature as far as useful or mandatory
- Reasonability check

G. Input Control

Measures to ensure that it is possible to check and establish whether and by whom personal data / social data have been entered, modified or removed into/from data processing systems.

- Automatic protocol of input, modification and deletion of personal data
- Protocol of the use of administration tools

- Protocol of system generation and modification of system parameters
- Complete protocol of all instances
- Revision secure protocol of access rights
- Protocol data can be analyzed in computer assisted processes
- Proof of the organisational defined responsibilities for input of data
- Definition of deletion and retention periods for the protocols
- Electronic signature (if applicable)

H. Job Control

Measures to ensure that, in the case of commissioned processing of personal data, the data are processed strictly in accordance with the instructions of the principal.

The following measures are relevant in case of sub-order for the subcontractor as well.

- Careful selection of the contractor (processor)
- Written agreement with definition of the decisional authority based on statutory mandatory law
- Outline of the rights and duties of principal and contractor in regard to:
- Data security measures
- Transmission directives
- Retention and deletion periods
- Insurance
- Definition of safety measures
- Right of access to subcontractor premises
- Control of security measures at the subcontractor
- Control of the correct execution of the contract
- Sanctions in case of contract violations

I. Availability Control

Measures to ensure that personal data is protected from accidental destruction or loss (e.g.: loss of power, lightning, protection from water damage)

- Ordinance of work instructions and safety directives
- Fire preventions
- Definition and control of fire precautions and fire/water early warning system
- Risk- and weak-point-analysis for relevant IT-division
- Intrusion detection and event notification
- Management procedures for incidents and events to enable appropriate investigation and resolution
- Safeguarding of the electric power supply by uninterruptible power supply
- Regular and intense instruction of all employees
- Disaster recovery plan, emergency handbook, security-infrastructure
- Recovery-Procedures for production data
- Data mirroring
- Regular stringent data back up
- Storage of back up media in safeguarded locations for production data (Data generated in Service Processes/Help Desk is deleted after the ticket is closed in due time)
- Instructions for documentation of procedures and software development
- Formalised approval process for new IT-applications and in case of relevant changes of running applications
- Used software is checked and released in a formalised procedure
- Centralized procurement for hard- and software
- Database-Logging
- Function separation between functional department and IT-division

J. Separation Control

Measures to ensure that data collected for different purposes can be processed separately.

- Stringent company internal directives for data collection, data processing and use of data
- Grant of specific access rights
- Use of separate user roles to ensure separation control
- Use of pseudonyms as far as possible and reasonable
- Documentation of data bases
- Documentation of application programs
- Documentation of the specific purposes of the collection, processing and use of data
- Instalment of logical databases
- Logical separation of data
- Physical separation of data