EXCEPTIONAL INNOVATION/QUADRIGA/INTERTOUCH

GLOBAL DATA PROTECTION POLICY

Introduction

ThIs Data Protection Policy provides the formal policy of the Quadriga interTouch family of companies (individually and collectively the "Company") concerning personal data and governs the data privacy and data protection practices and obligations of each Company and its workers. This Policy reflects both legal and contractual requirements applicable to the Companies, including the GDPR (setting forth privacy and data protection rules applicable to EU citizens), the Federal Trade Commission regulations (consumer privacy protections generally applicable to US-based companies), the data privacy and data security laws promulgated by the various countries, including governments of China, Australia and Canada, as well as the privacy and data security policies of the major hospitallity brands under the the terms of its respective master services agreements.

Purpose

The Company must comply with the data protection principles and requirements set out in relevant and applicable legislation, as well as comply with the privacy and data protection commitments set forth in the Company's agreements with the various hospitality brands. In order to harmonize disparate requirements and ensure compliance globally, we are adopting principles that adopt the most prescriptive standards applicable (regulatory or contractual) to our services and corporate conduct. This Policy applies to all personal data accessible, transmitted, collected, processed and/or stored by the Company in relation to its staff, service providers and customers in the course of its activities. The Company makes no distinction between the rights of data subjects who are employees, and those who are not. All are treated equally under this policy.

Scope

The policy covers all personal information (personally-identifiable information, as such term is generally understood and defined specifically defined in the agreements between the Company and major hospitality brands, as well as "personal data" as such term is defined under GDPR). The policy aplies equally to personal data held in manual and automated form.

This policy should be read in conjunction with associated policies (as may be centrally adopted or regionally adopted/applicable), including subject access request procedures, the Incident Response Procedure, the Acceptable Use Policy, the Data Retention and Destruction Policy, the procedures for granted and limiting administrative access to network systems and the corporate Code of Conduct (including requirements for compliance with law and protection of confidential information).

General Policy Statement

It is the policy of the Company that our practices affecting personal data will:

1. **Afford individuals the right to understand the personal data that we process and control the manner, extent and contined processing of personal data.** The General Counsel will formulate and distribute, from time to time, specific training and guidance on the scope of the duties of the Company on the rights of individuals and how the Company will comply with data subject access requirements and asertions of right to amend, erase, object to data

or port data. Our practices on the handling of personal data will ensure that individuals have:

- The right to be informed.
- The right of access.
- The right of rectification.
- The right to erasure of personal data.
- The right to restrict processing.
- The right to data portability.
- The right to object.
- The right to control automated decision-making and profiling.

2. **Reflect the legal and reputational concerns of our customers, demonstrate good stewardship and advance mutually-protective and beneficial objectives.**
    - We will ensure that our mutual obligations under the law, including GDPR, are reflected in our written agreements with our customers and fulfill the legal requirements for data protection applliable to both parties.
    - We will understand and comply with the directions and instructions of our customers pertaining to our processing of their data subjects that are guests receiving or interacting with our services and products
    - We will understand and comply with the general data privacy and data security requirements set forth in our master brand agreements and work collaberatively with our brand partners and ownership groups to ensure that our practices evolve with changing standards, regulatory requirements, and technology (both evolving risks and tools for mitigating such risk).
3. **Ensure that our procedures and standards for business operations incorporate security-by-design principles to ensure that data privacy and security are considered and prioritized in every area of our business.**
    - New projects or new areas of business will be subject to a data assessment and review coordinated by the Data Protection Officer.
    - New partners, service providers and other "subprocessors" will be subject to a data privacy and security due diligence process in order to ensure review and approval of data practices. Any disclosure of personal data to an entity or representative of an entity without execution of a Data Protection Addendum reviewed and approved by the General Counsel.
    - New products or modifications to existing products (including any integration of third party services) must include a review and approval by the Data Protection Officer to ensure that data privacy issues are identified and addressed as a necessary part of planning and design.
4. **Comply with corporate requirements for record-keeping (to ensure that data privacy and security issues are documented as a part of our corporate records) and managed in accordance with our records' retention policy requirements**.

Modification and Update

This policy shall be reviewed and updated, as appropriate, in response to a) changes to law or regulation, or binding interpretations thereof; b) improvements in data security technology and industry uses thereof; c) instances of preventable fraud and/or security breach; and d) annually in accordance with the annual risk assessment/update to the DPIA.

Third-Party Processors

In its relationship with Customers, the Company processes personal data as a "Processor" within the meaning of GDPR. In its relationship with third-party processors when the Company controls and

defines the protocols that will govern the handling of personal data, the Company acts in its capacity as a "Controller" within the meaning of GDPR.

When the Company engages a Data Processor to process personal data on its behalf, we must enter into an agreement with the Processor (a "Data Protection Addendum") which describes our instructions and requirements for the Third-Party Processor. This Data Protection Addendum outlines the obligations of the third-party Processor in relationship to personal data, the specific purpose for which they receive or access personal data, and their duty to process data in complinace with data protection laws (primarily GDPR) and our instructions. The form of Data Protection Addendum shall be approved by the General Counsel, along with any proposed modifications thereto. No employee may disclose personal data to any third-party without an executed Data Protection Addendum.

Data Security

The Company shall employ reasonable and legally-sufficient security measures to protect personal information, in transit and at rest. These measures for the Company's physical and electronic information systems will include ordinary and reasonable administrative, technical and physical safeguards, as set forth herein and otherwise supplemented by departmental and regional standards and procedures in order to preserve the privacy and integrity of personal information. All Company officers and employees are required to observe proper care in identifying, managing, security and maintaining the confidentiality of personal information.

1. **Limited access to personal information will be strictly controlled and monitored.** Only employees with a business need for access to personal data will be granted such access, and the degree of access shall correspond to that which is necessary to accomplish business functions, and access shall be modified or terminated as the degree of access necessary changes in accordance with altered job functions. The Information Security Officer shall conduct periodic reviews of Company systems to ensure that access to systems containing personal information is limited to employees for whom business needs justify access and that access is limited to only that personal information. Employees are prohibited from transmitting or sharing any personal information with other employees who do not have a business need to receive or access personal information under this Policy.

2. **Transmission of personal information shall utilize Company-approved methods of transfer (including the use of encryption technology, where applicable) and comply with Company limitations on cross-border transfers of personal data.** The Company shall adopt and continuously review standards to protect personal information in transit. No personal information on a citizen of an EU member state may be transferred via email or other insecure methods of transfer without approval from the Data Protection Officer. Any physical transfer of personal information shall be sent using a commercially recognized courier service or alternative secure mechanism that provides the capacity for tracking in transit and confirmation of delivery.

3. **Storage of Personal Data shall be limited to that which is necessary for business functions and supported by the consent of the data subject (the individual) or an alternative legitimate interest (which must be documented in the DPIA and approved by the General Counsel).**

    - All systems containing personal data shall be documented with the Information Security Officer. All personal information stored on removable electronic media shall be clearly labeled as "Confidential." No physical systems containing

personal data shall be moved from a secure location to an unsecure storage location without the approval of the Information Security Officer.
- All personal data stored on portable media or in physical form shall be stored in a locked room or filing cabinet.

4. **Unauthorized disclosure of personal data is prohibited.** No Company employee or representative may disclose personal information to a third party, whether such personal data is a part of an individual record or contained within a list, unless such disclosure has been authorized by the Data Protection Officer. Any request by a regulatory or law enforcement authority shall be immediately referred to the General Counsel for response.

    - No employee may shared or transfer, under any circumstances, any personal information via end-user messenging technologies, instant messaging, via social networking sites, though online chat spaces or through any other means not authorized by the Information Security Officer.
    - Wrongful disclosure includes transfer to or storage of personal data on employee-owned personal devices, including personal laptops or mobile devices. Employees are strictly prohibited from using their own personal devices in connection with personal data.

5. **Acceptance of Media used by a Customer that contains personal data is prohibited. No employee shall accept the return of media that has been provided for use by a customer, whether by sale or lease, which may contain personal data, for re-use or destruction, unless any and all personal information has been removed from such media**.

6. **Company systems shall maintain reasonable security measures to prevent unauthorized access to systems containing personal data**.

    a. Any system that contains personal information operated by the Company shall have the latest vendor-supplied security patches installed within 30 days of the date that the vendor makes such patches available.
    b. Any system that is owned and operated by the Company shall employ anti-virus software sufficient to detect, remove and protect against known viruses and are up-to-date with the capacity to generate audit logs.
    c. Any system containing personal information shall be segregated and accessible only via password in order to restrict access to authorized employees. The system shall maintain adequate firewall configurations to protect against unauthorized access of personal information by third parties via the internet.
    d. No personal information can be posted to a third-party online site (i.e. DropBox or similar services) unless authorized by the Information Security Officer.

7. **Review and Assessment.** The Data Security Officer and Data Protection Officer shall conduct a risk assessment at least once per year. The risk assessment should encompass all information systems that collect, store, transmit, process or facilitate access to personal information. The Company shall employ the NIST risk assessment or similar methodology.

8. **Incident Response, Notification and Harm Mitigation.** Upon the discovery or receipt of notice of any Security Incident, which shall include any violation of this Policy, including a circumstance of suspected or known fraudulent transaction or data breach. the Company will promptly implement response protocols as established by the Data Protection Officer and the Information Security Officer. The Data Protection Officer shall

be responsible for documenting the process and resolution of any Security Incident investigation, identifying any legally or contractually-required notification requirements and giving notice in accordance with such requirements within the timeframe set forth in the relevant agreement, statute or regulation.