Personal Information Privacy

V 1.0

Change log

Version	Date	Author	Reviewers	Approvers	Changes
1.0	9th December 2019	Jose Galdeano	Ellie Airey-Hoyland		Initial Document

Policy

During the ordinary course of business, Dominvs Group collects, processes, stores, and uses personal information (also referred to or described as personal data or personally identifiable information (PII) (collectively "Personal Information" or "PI") pertaining to our existing, potential, and former owners, customers, members, guests, and employees in order to provide world class service, meet our business objectives, and deliver benefits to
our employees. The Company is committed to respecting the privacy of its customers, potential customers, guests, employees and suppliers.
This Policy is designed to illustrate the Company's goal to comply with data protection laws in the countries in which Dominvs Group operates, to retain the trust of its owners, customers, members, potential customers, guests, and employees, and to process PI with confidence that consistent security and data protection controls are in place wherever Dominvs Group operates in general.

Applicability

This Policy applies to the Processing of Personal Information by electronic means and in systematically accessible paper-based (i.e. hard-copy) filing systems. This Policy applies to all Dominvs Group entities, properties and hotels. Each employee shall be responsible for his or her compliance with this Policy when handling PI.

Objectives

The main objectives of this Policy are to:
• Provide adequate and consistent data protection and privacy principles for the Processing of all Personal Information within Dominvs Group.
• Ensure that the processing of PI relating to existing, potential, and former owners, members, customers, guests, and employees conforms to the data protection principles set out in this Policy or related policies and standards
and meets the requirements of applicable data protection laws;
• Be able to respond promptly to the request of any existing, potential, and former owners, members, customers, guests, and employees exercising his or her rights under the applicable data protection laws.
• Ensure that all the representatives of Dominvs who deal with processing of PI relating to existing, potential, and former owners, members, customers, guests, and employees are aware of their responsibilities under applicable data protection laws. Personal Information Privacy and Processing Principles Processing, Process, or Processed means any operation that is performed on PI or on sets of PI, whether or not by automatic means, such as collection, recording, organization, storage, adaptation, alteration, retrieval, consultation, use (including in a different context), disclosure (including the granting of remote access), blocking, transmission, dissemination or otherwise making available, restriction, deletion, or destruction.
Dominvs Group respects the privacy rights and interests of each individual and will observe the following privacy principles.
• Privacy and data protection will be a key consideration in any project or technology involving PI.
• Personal Information will be:
◦ Processed transparently, fairly, and lawfully.
◦ Collected for specified, legitimate purposes and not Processed further in ways incompatible with those
purposes.
◦ Relevant to and not excessive for the purposes for which it is collected and used.

◦ Accurate and, where necessary, kept up-to-date. Reasonable steps will be taken to rectify or delete Personal Information that is inaccurate or incomplete.
◦ Kept only as long as is necessary for the purposes for which it was collected and Processed.
◦ Protected against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical and organizational measures.
◦ Processed in accordance with the individual's legal rights.
Personal Information is a category of Confidential Information broadly defined to include any information, regardless of the media on which such information is stored (e.g., on paper or electronically), related to a natural person (or data subject or data owner) that can be used to directly or indirectly to identify the person. PI includes, but is not limited to, the following:
◦ Name only
◦ Name (First or Middle Initial + Last)
◦ Address + other elements
◦ Telephone number
◦ Email address
◦ Credit history
◦ Certain room or travel preferences
◦ Internet Protocol (IP) address information (in certain jurisdictions)
◦ Geolocation information

There are many laws and regulations that govern the Processing or use of PI. Any access to and use of PI must be for authorized business purposes only and in accordance with such laws and regulations.
Senior management, in consultation with the Legal Department and the , should separately review and approve any nonroutine use of PI. Employees who routinely deal with PI should familiarize themselves with readily available Company policies and standards, training materials, such as the Information Security and Protection Training (ISPT), and applicable laws and regulations.
While the Processing of PI may vary depending on specific Company department rules and legal mandates, the following are the minimum requirements that must be met when Processing PI. Company departments should work with the
Information Technology (IT) Department to ensure these same principles are applied to secure exchanges of information
via systemic means by following all Information Security Standards.

• **Security and Confidentiality**
◦ PI must be treated as Company Confidential Information and will be subject to the security and related protections set forth in the Information Security and Confidentiality Policy

• **Use of Personal Information by Third Parties**
◦ PI is never to be sold, rented, licensed, exchanged or otherwise transferred to third-parties for their own use, including for their own marketing activities, without documented approval of the individual to whom the personal information pertains and express written permission from the legal department or a company director.

• **Use of Personal Information by Business Partners or Third-Party Service Providers**
◦ PI will only be shared with business partners or third-party service providers if there is a Company business need and such sharing is consistent with the reasonable expectations of the individual.
◦ Before PI is shared with business partners or third-party service providers, an impact assessment may be necessary and carried out in accordance with Company policies and procedures.
◦ The release of select PI necessary for the future operation of a business location upon the Company's termination of a management or other agreement may proceed with express written permission from the legal department or a company Director.

• **Use of Personal Information for Joint Marketing Activities** with Third Parties
◦ Joint marketing activities with third parties that involve PI may be proposed. Use of the information for these purposes is permissible with the applicable consent of the individual that the information pertains to and the express written permission from an attorney in the Law Department. Access to PI is not to be provided directly to such third parties except as specifically approved by the Director, , the Law Department and a company Director. In general, when conducting joint marketing activities with third parties, a third-party service provider should be used to conduct the marketing activities (*e.g.*, sending e-mails) so that the PI is not provided directly to the third party with which the Company jointly markets. PI should only be provided to third-party service providers under written agreements

that are approved by legal department and a company director, duly executed by a corporate officer, contain adequate security and confidentiality protections, and only to accomplish the Company's business purposes in a manner that is consistent with our privacy requirements.

• **Use of Personal Information by Company Department(s)**
◦ Prudent use of PI can help increase Company department sales and support; however, it is important to first consider (a) the purpose for which the information was originally collected, (b) the expectations and permissions of our existing, potential, and former owners, customers, members, guests, and employees Personal Information Privacy.
◦ A Company department requesting to use PI collected by another Company department must obtain the approval of the head of the department that collected and manages the desired information. That department head is responsible for ensuring that legal and regulatory requirements are satisfied, which includes consultation with ad company Director, and the Legal Department.

• **Company Websites**
◦ All Company websites that collect PI must include a link to the applicable online privacy statement of Dominvs Group or its affiliate, direct subsidiary, or indirect subsidiary, which have been reviewed and approved by a company Director and the in consultation with the Legal Department. A link to the applicable online privacy statement must be placed on the home page and every page on which PI is collected. All Company departments and functional areas must comply with such applicable online privacy statement as well as internal policies, procedures, and standards. Secured Sockets Layer (SSL) or equivalent encryption must be used on all web pages that collect PI.

• **Information on Web Servers**
◦ High Risk Information must not be stored on web servers. Web servers must function only as pass-through for transmission to a separate database on a separate network segment for financial PI such as credit card numbers. Connections from web servers to the Company's internal network are secured using appropriately configured firewalls. In addition, connections from Payment Card Industry (PCI) web servers to other Company servers are also secured via encrypted transmission.

• **Direct Marketing**
◦ It is the Company's objective to respect the wishes of existing, potential, and former owners, customers, members, guests, and employees (i.e. employees) regarding whether or not they desire to receive direct marketing materials from the Company. Certain jurisdictions permit direct marketing only with the consent of the individual that will receive the marketing message. The Company will comply with all legal requirements relating to any direct marketing activity. Company departments must consult with the Director and the Law Department to review the overall planned approach for the direct marketing activities by category (e.g., e-mail, print mail), prior to engaging in such activities, to verify that they comply with applicable laws.

• **Compliance with Requests from Law Enforcement Agencies**
◦ It is expected that the Company will occasionally receive requests for PI pertaining to owners, customers, members, guests, or employees (i.e. employees) as part of an investigation or legal proceeding. As a general matter, the Company will disclose PI without the permission of the guest or employee when required by law, or in good faith that such action is necessary to investigate or protect against harmful activities to the Company's owners, members, customers, prospects, guests, employees, property, or to others.

• **Collection and Use of Sensitive Information or "Special Categories of Personal Data"**
◦ "Sensitive Information" or "Special Categories of Personal Data" is Personal Information concerning racial or ethnic origin, political opinions, religious affiliations, philosophical or moral beliefs, labour union membership, and information concerning health conditions, sexual habits, or behaviour. You may not request, collect, or retain Sensitive Information or Special Categories of Personal Data without the prior approval Dominvs Group , the legal Department, and the company directors, along with the applicable consent of the individual (data subject) in accordance with current laws and regulations worldwide.

• **Nonproduction (Lower) Environments**
◦ PI that is restricted from nonproduction environments includes, but is not limited to credit card Information, Government Issued IDs (such as National Insurance / Passport / Driver's License), and Health and Medical related Information.

• **Non-public Personal Information (NPI)**
◦ The protection of Non-public Personal Information (NPI) is a vital component of the Company's operations, culture and policies, including, but not limited to, in connection with its mortgage banking operations.

• **Additional requirements and Procedures**
◦ Because privacy laws vary by country, additional measures may need to be deployed to satisfy those laws as they apply to the Company. This Policy does not replace or supersede any obligations under existing privacy laws, and the various data protection laws in the EU.

Personal Information Owners and Stewards

Information Owner

Each information asset and data set must have a designated information owner. Information owners are key business leaders who "own" risk accountability for the information their processes rely on. They are accountable for ensuring the information is appropriately created, gathered, and maintained, but do not necessarily deal with the day-to-day handling of the information. Information owners are the department heads or directors in the company.
In the case of PI, the information owner is accountable for the determination of the purpose and means of processing in accordance with the privacy notices provided and the security guidelines. While the information owner is ultimately accountable for the protection of that information, they may delegate responsibility to an information steward to act on their behalf.

Information Steward

An information steward, appointed by the information owner, is responsible for ensuring effective control and use of data assets and exercising a series of functions assigned to them by the information owner or governance organization.
This may include assigning classification levels, determining protection requirements, and communicating the access rules and information protection requirements to appropriate parties, such as IT. Information stewards are typically management positions within the business area that have expertise/knowledge of the information and how it should be handled.
In the case of Personal Information, the information steward insures the processing according to the notices and consent provided.
Additional Responsibilities of Employees when Handling PI
In addition to the Privacy and Processing Principles set forth in this Policy, each employee whose job responsibilities include setting direction for or to directly collect, manage, or dispose of PI is required to:
• understand all applicable policies and standards;
• complete applicable training on the handling of PI and NPI;
• minimize the information collected only to that which is necessary for the specific business purpose;
• limit access to the information to only those individuals with a business need to know;
• protect the information that is collected;
• when handling requests from law enforcement or similar entities, direct inquiries Legal Department.
• securely dispose of the information when it is no longer required for business purposes in accordance with the IT Department's processes.
• protect electronic resources that provide access to the information.
If you become aware of any violation of this Policy:
• Promptly contact the IT Department and the legal department with any questions or concerns about noncompliance or to report suspected violations of this Policy.
• Please note that any violation of any of the requirements in this Policy can result in disciplinary action up to and including termination.