Privacy Policy

Version 7.0
January 2020

Disclaimer

All information in this document is subject to change without notice. Although the information is believed to be accurate, it is provided without guarantee of complete accuracy and without warranty of any kind. It is the user's responsibility to verify and test all information in this document and the user accepts full responsibility for all resulting outcomes.

Trademarks

SRSTP, UCMP-RIG, UCMP-DA, UCMP-CA, Converged Management Platform, UCMP, Vendor Knowledge Module, VKM, Vendor Quality Module & VQM are trademarks of Nectar Services Corp.

Microsoft, Internet Explorer, Windows, Windows Server, Windows Vista, Win32, and the Microsoft logo, Windows logo, Windows logo (2002), Internet Explorer logo, Lync Logo and Windows start button, are registered trademarks. Lync 2010, Lync 2013, Skype for Business, Windows XP, Windows 2008, Windows 2010, Windows 2012, and Windows 2016 are trademarks of Microsoft.

CentOS Marks (CentOS 6 and CentOS 7) are trademarks of Red Hat, Inc.

Oracle, Oracle logo, Java, Solaris, all trademarks and logos that contain Oracle, Solaris, or Java, and certain other trademarks and logos, are trademarks or registered trademarks of Oracle Corporation or its subsidiaries in the United States and other countries.

Cisco, Cisco Unified Communications Manager, Cisco Call Manager Express, Cisco Unity, Cisco Unity Express, Cisco Unified Border Element, are registered trademarks. Cisco UCM, Cisco CME, Unity, Unity Express, and CUBE, are trademarks of Cisco.

Avaya and the Avaya logo are trademarks of Avaya Inc. and may be registered in certain jurisdictions.

NICE Trading Recording is a trademark of NICE Systems.

Unigy is a registered trademark of IPC Systems, Inc.

FreeBSD and the FreeBSD logo are registered trademarks to The FreeBSD Foundation.

Sonus and Sonus logo are registered trademarks of Sonus Networks, Inc.

All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

Approvals

Owner	Title	Date	Signature
James E. Gerb	Data Protection Officer	May 2, 2018	
James E. Gerb	Data Protection Officer	January 8, 2019	
James E. Gerb	Data Protection Officer	January 1, 2020	

Approved By	Title	Date	Signature
Marshall W. Rosenthal	General Counsel	May 2, 2018	
Marshall W. Rosenthal	General Counsel	January 8, 2019	
Marshall W. Rosenthal	General Counsel	January 1, 2020	

Document History and Version Control

Version	Date	Author	Revision Notes	Section
1.0	December 2013	Anthony Fernandez	Initial Policy Draft	All
1.1	January 2014	Anthony Fernandez	Final Policy	All
2.0	January 2015	Anthony Fernandez	Annual Review, updated and release	All
3.0	January 2016	J.E. Gerb	Annual Review, updated and release	All
4.0	January 2017	J.E. Gerb	Annual Review, updated and release	All
5.0	January 2018	J.E. Gerb M. Rosenthal D. Martinez	Annual Review, updated and release	All
5.1	May 2018	J.E. Gerb D. Martinez	Compatibility with GDPR; added section 11.	1, 2, 3, 11
6.0	January 2019	J.E. Gerb M. Rosenthal	Annual Review, updated and release	All
7.0	January 2020	J.E. Gerb M. Rosenthal	Annual Review, updated and release	All

Table of Contents

1. Purpose

In the course of its business, it is necessary for Nectar Services Corp. (hereinafter, "Nectar") to record, store, process, transmit, and otherwise handle private information about individuals. Nectar takes these activities seriously and provides fair, secure, and fully legal systems for the appropriate handling of this private information. All such activities at Nectar are intended to be consistent with both generally accepted privacy ethics, standard business practices, and the General Data Protection Regulation (GDPR) enforced in the E.U.

2. Scope

This policy applies to all Nectar employees and contractors who handle private information about individuals, either affiliated with Nectar or having no affiliation. In protecting the personal data of these individuals, Nectar follows the principles, rules and obligations imposed by GDPR.

Within this Policy we use the following terms:

- 'private information' or 'personal data' means any information relating to an identified or identifiable individual.
- 'individual' refers to a natural person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
- 'handling' or 'processing' means any operation or set of operations which is performed on personal data, such as access, collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Some frequently occurring examples of identifying personal data are:

- Names, home addresses, phone numbers, social security numbers.
- IP addresses, cookies, geo-location coordinates.
- email addresses, LinkedIn ad other social media addresses.

3. Management Responsibilities

Management must take appropriate technical and organizational measures to ensure and to be able to demonstrate that processing of personal data of an individual is performed in accordance with the following principles:

a. It is processed lawfully, fairly and in a transparent manner in relation to the individual.

b. It is collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

c. It is adequate, relevant and limited to what is necessary in relation to the purposes.

d. It is accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which they are processed, is erased or rectified without delay.

e. It is kept in a form which permits identification of individuals for no longer than is necessary for the purposes for which the personal data is processed.

f. It is processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures.

4. Disclosure Of Private Information

4.1 Revealing Information About Policies and Procedures

As a general rule, information security policies and procedures should be revealed only to Nectar workers and selected outsiders, such as auditors, who have a legitimate business need for this information. A notable exception involves the policies that deal with private information about individuals. All involved individuals have a right to receive an officially approved statement of Nectar policies and procedures regarding the handling of information about them. In addition, Nectar must disclose the existence of systems containing private information and the ways that this information is used. With the exception of criminal and policy-violation investigations, there must be no system of personnel records within Nectar whose very existence is kept secret from the people described therein.

4.2 Handling Private Information Requests

All requests for private information coming from a person or organization outside Nectar must be forwarded to the Nectar Chief Legal Officer or corporate legal counsel. All requests for private information that fall outside normal business procedures and that come from a Nectar insider must be forwarded to the Director of the Human Resources Department. These Managers will decide whether the requests will be granted.

5. Appropriate Handling Of Private Information

5.1 Collect Only Necessary Information

In general, Nectar may collect, process, store, transmit, and disseminate only that private information that is necessary for the proper functioning of its business. For example, Nectar Management must not collect information about worker activities during non-work hours unless these activities are highly likely to influence the involved worker's performance, or unless they could adversely affect the reputation of Nectar.

5.2 Destruction Of Private Information

When private information is no longer needed, it must be destroyed by shredding, or by other destruction methods approved by the Information Security Department. Destruction of private information resident on computer disks and other magnetic media must be accomplished with an overwriting process. A simple erase process is not sufficient. To assure the proper destruction of private or confidential information, disposal of computers with embedded hard disk drives or other data storage systems must proceed according to procedures issued by the Information Security Department.

5.3 Removal Of Private Information

Private or Confidential information must not be removed from Nectar offices. Permission to take such information offsite may be granted by a Departmental Manager provided the involved worker has completed the information security segment of telecommuter training, and passed the associated test. Signed third-party on-disclosure agreements may additionally be required when private information is removed from Nectar offices. Private information must not be moved to another country unless the permission of the Manager of the Information Security Department is obtained.

5.4 Preventing Inadvertent Disclosure on Screens

The display screens for all personal computers, workstations, and dumb terminals used to process sensitive or valuable data, including private information, must be positioned such that they cannot be readily viewed through a window, by persons walking by a hallway, or by persons waiting in reception and related areas.

5.5 Preventing Inadvertent Disclosure By Hardcopy

Whenever a worker is handling private information, if a person who is not authorized to view that information enters the immediate area, steps to conceal the information must promptly be taken. If the information is in physical form, the information can be covered with other material. If the information is displayed on a computer screen, the worker can invoke a screen saver or log off.

6. Private Information On Computer And Communication Systems

6.1 Expectation Of Privacy

All messages sent over Nectar internal computer and communications systems are the property of Nectar. Management reserves the right to examine all information transmitted through these systems. Examination of such information may take place without prior warning to the parties sending or receiving such information. Because the Nectar computer and communications systems must be used for business purposes only, workers must have no expectation of privacy associated with the information they store in or send through these systems.

6.2 Examination Of Stored Information

At any time and without prior notice, Nectar Management reserves the right to examine archived electronic mail, private file directories, hard disk drive files, and other information stored on Nectar information systems. Such examinations are typically performed to assure compliance with internal policies, support the performance of internal investigations, and assist with the Management of Nectar information systems.

6.3 Manager Involvement In Monitoring

Whenever a worker's computer or communications user ID is monitored for investigative or disciplinary purposes, the involved worker's Manager must be informed of this activity promptly. All worker monitoring must itself be logged for subsequent Management review and possible use in disciplinary or legal actions.

6.4 Department Manager Activity Review

Nectar routinely logs web sites visited, files downloaded, and related information exchanges over the Internet. Nectar records the numbers dialed for telephone calls placed by each worker. Department Managers routinely receive reports detailing the usage of these and other internal information systems, and are responsible for determining that such usage is both reasonable and business-related.

6.5 Changing Information Resident on Systems

Management reserves the right to delete, summarize, or edit any information posted to Nectar computers or communication systems. These facilities are privately-owned business systems, and not public forums, and as such do not provide free-speech guarantees.

6.6 Routine Usage of Backup Systems

All files and messages stored on Nectar systems are routinely copied to tape, disk, and other storage media. This means that information stored on Nectar information systems, even if a worker has specifically deleted it, is often recoverable and may be examined at a later date by system administrators and others designated by Management.

6.7 Remote Computer Monitoring

Nectar routinely scans the personal computers connected to its networks. These scans ensure that remote computers are operating only with approved and licensed software, are free from viruses and worms, and have been used only for approved business purposes.

6.8 Encryption Of Electronic Mail

Workers must consider electronic mail to be the computerized equivalent of a postcard. Unless material sent by electronic mail is encrypted, workers must refrain from sending credit card numbers, passwords, research and development information, medical histories, computer programming source code, and other private or confidential information through electronic mail.

6.9 Links Between Separate Types Of Private Data

Without advance consent from the Manager of the Information Security Department, Nectar information systems must not be configured to support new links between private information and other types of information related to the same individual.

7. Activity Monitoring

7.1 Physical Security Systems

Workers may be subject to electronic monitoring of their activities while on Nectar premises. This monitoring is used to measure worker performance and to protect worker private property, worker safety, and Nectar property. In areas where there is a reasonable expectation of privacy, such as bathrooms, dressing rooms, and locker rooms, no electronic monitoring will be performed.

7.2 Personal Effects and Private Communications

All personal effects brought to Nectar premises are subject to search at any time without advance notice. Workers wishing to keep certain aspects of their personal life private must not bring related personal effects to Nectar premises. To keep these matters private, workers must not communicate about such matters using Nectar telephones, electronic mail systems, or other communications systems that maybe monitored and which are intended to be used for business purposes only.

7.3 Use Of Informants

From time to time, Nectar uses informants who may be placed in various internal positions and who may appear to be the same as any other worker. Management has no obligation to notify workers about the presence of, or nature of the work performed by, such informants.

7.4 Pretext Requests

Nectar believes that all business activities must be conducted in a forthright and honest manner. However, in certain circumstances authorized by the Director of Physical Security, the organization may utilize investigators who pose as other persons in order to test customer service, test security policies, or investigate alleged wrongdoing.

8. Handling Personnel Information

8.1 Access to Own Personnel File

Upon written request, every worker must be given access to his or her own personnel file. Employees must be permitted to both examine and make one copy of the information appearing in their personnel file. If employees object to the accuracy, relevance, or completeness of information appearing in their personnel file, each year they may add a supplementary statement of up to 200 words.

8.2 Disclosure To Third Parties

Disclosure of private information about Nectar workers to third parties must not take place unless required by law or permitted by explicit consent of the worker. Nectar must not disclose the names, titles, phone numbers, locations, or other contact particulars of its workers unless required for business purposes. Exceptions will be made when such a disclosure is required by law or when the involved persons have previously consented to the disclosure. The reason for termination of workers must not be disclosed to third parties. Two permissible exceptions are the prior approval of a Nectar Senior Manager or if the disclosure is required by law. The Human Resources Department must record every disclosure of private information to third parties and these records must be maintained for at least five years.

8.3 Summary Of Disclosures

If they request it, workers must be provided with a summary of all disclosures of their private information to third parties. In addition, workers must be given sufficient information to permit them to contact such third parties to rectify errors or supply additional explanatory information.

8.4 Change Of Status Information

Detailed worker change of status information is strictly confidential, and must not be disclosed to anyone except those people who have a genuine need to know. Detailed change of status information includes the reasons for terminations, retirements, resignations, leaves of absence, leaves of absence pending the results of an investigation, inter-departmental transfers, relocations, and changes to consultant or contractor status.

9. Private Information From Job Seekers

9.1 Gathering Unnecessary Information

Private information about a prospective employee may not be gathered unless it is both necessary to make an employment decision and also relevant to the job. This policy addresses marital status, family planning objectives, off-hours activities, political affiliations, performance on previous jobs, previous employers, credit history, education, and other personal details.

9.2 Credit And Background Checks

Whenever a credit report will be examined or a background check will be performed, prospective workers must provide a written release indicating their approval of the process. These prospective workers must be given an opportunity to withdraw their application for employment or contract work if they choose not to disclose such private information to Nectar.

9.3 Permissible Tests

Candidates for a job with Nectar shall be subject to drug tests; however, candidates shall not be subject to AIDS tests, psychological tests, or other tests that may illuminate the candidates' lifestyle, political associations, or religious preferences.

10. Private Information About Customers

10.1 Consent for Collection Required

The collection of private information on prospects, customers, and others with whom Nectar does business, is customary and expected. However, Nectar workers must not collect private information from prospects or customers without having obtained their knowledge and consent.

10.2 Consent for Uses Required

Before a customer places an order or otherwise discloses private information, all Nectar representatives must inform the customer about the ways that this private information will be used, and the third parties, if any, to whom the information will be disclosed.

10.3 Collection of Unnecessary Information

Nectar workers or information systems must never require the provision of prospect or customer private information that is unnecessary for the provision of information, for the completion of a transaction, or for the delivery of products or services. No product or service provided by Nectar may be denied to any person if they refuse to provide unnecessary private information. All disputes about necessary private information will be resolved by the Nectar Chief Legal Officer or corporate legal counsel.

10.4 Opting Out from Unsolicited Contacts

Nectar customers must be given an opportunity to inform Nectar that they do not wish to be contacted through unsolicited direct mail, telemarketing, and related promotions. Nectar staff must faithfully observe and act on these customer requests. Nectar workers must diligently observe the unconditional right of individuals to block data about them from being included in mailing lists or calling lists, block the sale of data about them to third parties, and to have data about them erased from direct marketing lists.

10.5 Sharing of Customer Information

Nectar does not disclose specific information about customer accounts, transactions, or relationships to unaffiliated third parties for their independent use, except under certain circumstances. These circumstances are limited to the disclosure of information to a reputable information reporting agency such as a credit bureau, when performing its own due diligence related to a customer's request to perform a certain action such as extend the amount of an existing line of credit, those circumstances when the customer requests the disclosure, the disclosure is required by or permitted by law, or the customer has been informed about the possibility of such a disclosure for marketing or similar purposes, and has been given an
opportunity to decline.

10.6 Change of Business Structure

Should Nectar go out of business, merge, be acquired, or Nectar otherwise change the legal form of its organizational structure, Nectar may need to share some or all of its customer information with another entity in order to continue to provide products and services. If such a change and associated information transfer takes place, customers must be promptly notified.

10.7 Use of Outsourcing Organizations

Nectar may outsource some or all of its information handling activities, and it may be necessary to transfer prospect and customer information to third parties to perform work under an outsourcing agreement. In all such cases, the third parties involved must sign a confidentiality agreement prohibiting them from further dissemination of this information and prohibiting them from using this information for unauthorized purposes.

11. Private Information About Individuals

Nectar has adopted high standards of protecting the personal data of individuals that it does not have a direct business relationship with, such as personal data processed by the systems of its corporate clients that Nectar is either, operating or supporting.

Nectar employees and contractors will only process personal data when they are explicitly instructed to do so, in writing, by the corporate client, and they will strictly follow the instructions of the corporate client. Under no circumstances will Nectar employees or its contractors attempt to process the following types of personal data without the prior written consent and instructions of the corporate client, to wit:

- seeking access to personal data that they are not authorized to access.
- asking for or opening computer files, messages, or other media that may be expected to contain personal data.
- sharing screens that display personal data with unauthorized individuals.
- providing personal data in computer files, messages, or other media to unauthorized individuals.
- letting unauthorized individuals participate in video-conferences where personal data is shared, or is expected to be shared.
- letting unauthorized individuals gain access or otherwise involve them in personal data processing.
- recording video-conferences, making copies of personal data in any other way.
- accessing production databases, systems or log files.
- altering or destroying files, databases, printed documents that may contain personal data.
- starting or stopping computer systems that are involved in personal data processing.
- altering security, access control or permission mechanisms that change expose of personal data.

When Nectar employees and/or contractors either engage in, or are exposed to, personal data that they thereafter realize is unauthorized by a corporate client, such employee or contractor will immediately terminate the processing (terminate screen sharing, stop examining computer files, and perform other actions as appropriate) and will inform Nectar management of the unauthorized processing.

12. Violations

Any violation of this policy may result in disciplinary action, up to and including termination of employment. Nectar Services Corp. reserves the right to notify the appropriate law enforcement authorities of any unlawful activity and to cooperate in any investigation of such activity. Nectar does not consider conduct in violation of this policy to be within an employee's or partner's course and scope of employment or service, or the direct consequence of the discharge of the employee's or partner's duties. Accordingly, to the extent permitted by law, Nectar reserves the right not to defend or pay any damages awarded against employees or partners that result from violation of this policy.

Any employee or partner who is requested to undertake an activity which he or she believes is in violation of this policy, must provide a written or verbal complaint to his or her Manager, any other Manager or the Human Resources Department as soon as possible.

13. Definitions

Confidential Information (Sensitive Information) – Any Nectar Services Corp. information that is not publicly known and includes tangible and intangible information in all forms, such as information that is observed or orally delivered, or is in electronic form, or is written or in other tangible form. Confidential Information may include, but is not limited to, source code, product designs and plans, beta and benchmarking results, patent applications, production methods, product roadmaps, customer lists and information, prospect lists and information, promotional plans, competitive information, names, salaries, skills, positions, pre-public financial results, product costs, and pricing, and employee information and lists including organizational charts. Confidential Information also includes any confidential information received by Nectar from a third party under a non-disclosure agreement.

Electronic Messaging System – Any device or application that will provide the capability of exchanging digital communication between two or more parties. Examples are electronic messaging, instant messaging, and text messaging.

Information Asset – Any Nectar Services Corp. data in any form, and the equipment used to manage, process, or store Nectar data, that is used in the course of executing business. This includes, but is not limited to, corporate, customer, and partner data.

Objectionable Information or Material – Anything that is considered offensive, defamatory, obscene, or harassing, including, but not limited to, sexual images, jokes and comments, racial or gender-specific slurs, comments, images or jokes, or any other comments, jokes, or images that would be expected to offend someone based on their physical or mental disability, age, religion, marital status, sexual orientation, political beliefs, veteran status, national origin, or ancestry, or any other category protected binational or international, federal, regional, provincial, state, or local laws.

Partner – Any non-employee of Nectar Services Corp. who is contractually bound to provide some form of service to Nectar.

Password – An arbitrary string of characters chosen by a user that is used to authenticate the user when he attempts to log on, in order to prevent unauthorized access to his account.

User – Any Nectar Services Corp. employee or partner who has been authorized to access any Nectar electronic information resource.

14. References

ISO 27002 – 15.1.4 Data protection and privacy of personal information.

15. Related Documents

None.