NECTAR'S COMPLIANCE WITH THE EUROPEAN UNION'S GENERAL DATA PROTECTION REGULATION (GDPR)

Every Conversation Matters

ADDRESS

366 North Broadway
Suite 201
Jericho, NY 11753

1.888.811.8647

PREPARED BY:

James E. Gerb, V.P. and
Data Protection Officer
Nectar Services Corp.

Date of Issue: Jan 11, 2019

Revision: 5.0

Revision Date: January 6, 2020

TABLE OF CONTENTS

DOCUMENT CONTROL

REVISION HISTORY

NAME	DATE	VERSION	DESCRIPTION
JAMES E. GERB – V.P.	January 11, 2019	1.0	
MARSHALL ROSENTHAL – GENERAL COUNSEL	January 11, 2019	1.0	
JAMES E. GERB – V.P. ***RUSSELL WIANT – V.P. DEVELOPMENT***	May 28, 2019	2.0	Updated to include: Nectar 10, Perspective & Technical Notes
MARSHALL ROSENTHAL – GENERAL COUNSEL	May 31, 2019	2.0	Legal Review
RUSSELL WIANT – V.P. DEVELOPMENT	June 24, 2019	3.0	Additional Updates to technical Notes
JAMES E. GERB – V.P.	July 23, 2019	4.0	Updates: *Nature of Processing* – hosting info
MARSHALL ROSENTHAL – GENERAL COUNSEL	August 22, 2019	4.0	Legal Review
JAMES E. GERB – V.P. & MARSHALL ROSENTHAL – GENERAL COUNSEL	September 21, 2019	4.1	Additional updates & Legal Review
JAMES E. GERB – V.P. & MARSHALL ROSENTHAL – GENERAL COUNSEL	January 6, 2020	5.0	Annual review

1. NATURE AND PURPOSE OF PROCESSING

Nectar Services Corp. ('Nectar') was fully compliant with the European Union's (EU) General Data Protection Regulation (GDPR) upon its effective date of May 25, 2018, including the appointment of a Data Protection Officer (DPO) and EU Representative. Accordingly, Nectar's DPO contact information, EU Representative and Privacy Notice is posted on its website (https://www.nectarcorp.com/).

The personal data processing performed by the Nectar UC software is an integral part of the personal data processing performed by our global clientele operating communications infrastructure. This technology is NOT high risk to the privacy rights and freedoms of individuals (*see Sec. 4.0 below - Compliance with Data Privacy Rights of Individuals*).

Personal data processing performed by Nectar is NOT aimed at the data subjects but at the communication technologies they are using. The personal data used in the processing is limited to non-sensitive contact information meta data (e.g. name, phone number, email address and IP address) of the data subjects and limited details of their terminating equipment. And it is NOT specifically used for any special categories of personal data or data known to be about children or vulnerable individuals.

It is important to note that Nectar does NOT have any access to its Customer's Confidential information or data, nor any other Personal Data other than what is set forth above.

As mentioned above, Nectar is processing non-sensitive contact information meta data and NOT the content of voice and video calls generated by data subjects for investigating and resolving call quality issues. The processing reflects what has occurred in the target communications systems (e.g. Skype for Business, IP PBXs, Video platforms, headsets, etc.). The personal data is loaded from the target system into the Nectar UC software and quickly abandoned (retention time by default – 28 days). Again, the processing itself is targeted at communications infrastructure, NOT the data subjects, and is only visible to a very limited number of privileged engineers/administrators responsible for IT support.

Nectar uses personal data to only diagnose problems, advise its Clients and/or for the development of internal product improvements. And, the data ultimately needed to resolve support issues is very limited, affecting a very limited share of overall support related requests received by Nectar.

Nectar (as Processor) does NOT host the Nectar UC software at any of its global locations for the purpose of processing its Customer's (as Controller) provided personal data. Rather, Nectar provides its UC software to its Customers to either host on their premises or, alternatively, Nectar's UC software can be provided to its Customer's as a software as a service (SaaS) solution.

If the Customer choses to host the Nectar UC software on its premises, on their own infrastructure, then the Customer is solely responsible for physical and network security including access control to the Nectar UC software.

If the Customer choses the SaaS solution, then the Nectar UC software will be hosted at an Amazon Web Services (AWS) location accordingly. AWS has multiple compliance and certifications including but not limited to SOC 2, ISO 9001, ISO 27001, and ISO 27101 (cloud- specific information security controls). AWS is GDPR compliant as well. Please refer to https://aws.amazon.com/compliance/programs/ for all AWS compliance and certifications.

And, Nectar does NOT sell or share for monetary or other consideration, any personal data it collects (e.g. business contact data) in pursuit of its legitimate business interests to third parties.

2. DEFINITION OF ROLES

- ***Controller*** *- Client (channel partner or direct client)*
  - *Determines the purpose and means of processing*
    - *Personal data is only processed on documented instructions (to Processor)*
    - *Decides/provides data to be processed, choses specific configurations, defines reports, data exports, and further data usage.*
- ***Processor*** *- Nectar Services Corp.*
  - *Processes data on behalf of the Controller, acting on the instructions of the Controller.*
- ***Cloud Service Provider (CSP)*** *(if applicable)*
  - *The CSP will process personal data, which is on their servers, on behalf of the controller.*
    - *The CSP cannot do anything with the data*
    - *The data is owned by the Controller*
- ***Sub Processor*** *- any subcontractor engaged by Nectar for the processing of personal data.*
  - *Sub Processor employees are subject to same contractual obligations that are imposed on Nectar as Processor*
  - *Must develop and implement internal procedures and practices to protect personal data.*
  - *Requires specific written consent of the controller*

3. TECHNICAL AND ORGANIZATIONAL MEASURES

Nectar has implemented appropriate technical and organizational measures to ensure and be able to demonstrate that its processing is performed in accordance with GDPR. This includes annual review of the technical and organizational measures on effectiveness and acceptability.

3.1 ORGANIZATIONAL SECURITY MEASURES (ALL POLICIES / PROGRAMS REVIEWED ANNUALLY AT MINIMUM)

- ***Data Processing Agreement (DPA) – GDPR compliant agreement used by Nectar:***
  - *Asserts that only the personal data (e.g. non-sensitive contact meta data) needed to perform the Nectar UC software function are collected by the software from the client's infrastructure and nothing more, and that there is NO "special" data, which are defined as those revealing things like race, ethnicity, political conviction, religion, and more.*
- ***Nectar Third Party Security Management Policy:***
  - *Personal data collected in the scope of Nectar's cloud offering and support operations may, on a very limited basis, be transferred to US, UK and its sub processor in India.*
  - *Nectar uses Standard Contractual Clauses (SCC) which have data protection provisions built in as legal basis for international data transfers – also installed in DPA mentioned above.*
  - *Personal data shared during support calls is NOT further processed in any way by the side that provides the support.*
- ***Nectar Information Security Policy***
- ***Nectar Privacy Policy***
- ***Nectar Acceptable Use of Assets Policy***
- ***Nectar UCMP Operations and Support Guide***

- ***Nectar's Human Resources (HR) related programs and policies including:***
  - *Employee Security Awareness Program*
  - *Employment Contracts and its NDAs,*
  - *Employee Handbook including Nectar Code of Conduct and Employee Personal Liability clause*
  - *Nectar's signed Employee Annual Statement of Confidentiality*
  - *Non-Disclosure, Non-Competition and Adherence to the Nectar Employee Handbook and Nectar's Conduct, Employment and Security Policies.*
  - *Anti-Money Laundering (AML) Policy*
  - *Anti-Corruption Policy*
  - *Code of Business Conduct and Ethics Policy*

In addition, all Nectar employees are subject to civil and/or criminal prosecution for violation of said Nectar policies.

3.2 TECHNICAL SECURITY MEASURES (ALL POLICIES/PROCEDURES REVIEWED ANNUALLY AT MINIMUM)

- ***Access Controls:***
  - *Require logging in*
  - *Role-based privileges*
  - *Password strength policy for local accounts*
  - *Access limitation using VPN with restricted set of IPs*
  - *Limited number of authorized staff with access*
- ***Audits: (see Section 5.0 below – Technical Notes)***
  - *These logs can be accessed by system administrators revealing:*
    - *Audit log of log-ins*
    - *Location of log-ins*
    - *Data modified*

- ***Encryption:***
  - *Current Software Release - data encryption in transit only using TLS 1.2*
    - **Please Note:**
    - *Nectar 10 software release (cloud-based Solution)*
      - *Data in transit using TLS 1.2 encryption*
      - *Data at rest using AES 256-bit encryption*
    - *The Nectar Customer Experience (CX) Assurance family of products (which includes the product formerly known as Perspective) do NOT process any personal data.*
    - *Anonymization*
      - *Available on Unified Communications Diagnostics (UCD) and Call Analysis Module (CAM)*
- ***Retention:***
  - *Nectar UC software – 28 days of data (by default)*
  - *Internal Systems:*
    - *All personal data is deleted or returned (upon written request) once the provision of services is completed.*
    - *Support tickets are retained for three (3) years then deleted.*
- ***Data Breaches:***
  - *In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.*
  - *The processor shall notify the controller without undue delay after becoming aware of a personal data breach.*
  - *Nectar provides audit log functionality to aid in investigating a potential data breach.*
  - *Nectar Support Staff are all ITIL certified and adhere to ITIL best practices framework for service delivery, including Incident, Problem and Change Management.*

4. COMPLIANCE WITH DATA PRIVACY RIGHTS OF INDIVIDUALS

4.1 RIGHT OF ACCESS

Nectar provides scripts that system administrators can execute to automate a "right of access" response. There is not a self-service function made available to the data subject and not legally required as Nectar is not in contact with the data subject. Nectar UC software processes user directory data, obtained, from the target communications systems, reloaded frequently. And, the Nectar UC software does NOT store additional personal data that may need to be returned to the data subject.

4.2 RIGHT OF RECTIFICATION

Rectifiable personal data is mostly loaded in the Nectar UC software from the target communication systems, reloaded regularly and frequently, daily or even immediately, providing the right automatically.

4.3 RIGHT TO ERASURE (A/K/A RIGHT TO BE FORGOTTEN)

Nectar supplies scripts that system administrators can execute to automate a "right to erasure" request to erase data about a specific individual.

4.4 RIGHT TO DATA PORTABILITY

This is supported as described in the Right to Access above. Scripts allow system administrators to make a dump / export of all personal data and destroy it. However, this is not deemed applicable to the Nectar UC software and its use by global clientele.

5. TECHNICAL NOTES

For more information on how to enable auditing to prepare for GDPR, please refer to one of the following:

- *Nectar Foundation Central Intelligence Platform (CIP) Install/Upgrade Guide*
- *Nectar Foundation CIP/EIP Administration Guide*
- *Nectar Foundation RIG Administration Guide*
- *Nectar Foundation Perspective Administration and User Guide*
- *Software Release notes*

Please Note: Existing clients must upgrade their Nectar software to 'Release 7.2 or later' (CIP, EIP, RIG, Perspective Agent/Controller as well as the Nectar Foundation Client) to enable the new General Data Protection Regulation (GDPR) audit logging.

Logging is enabled by default but can be customized to suit your specific auditing needs. ***Please refer to Software Release Notes for further information.***