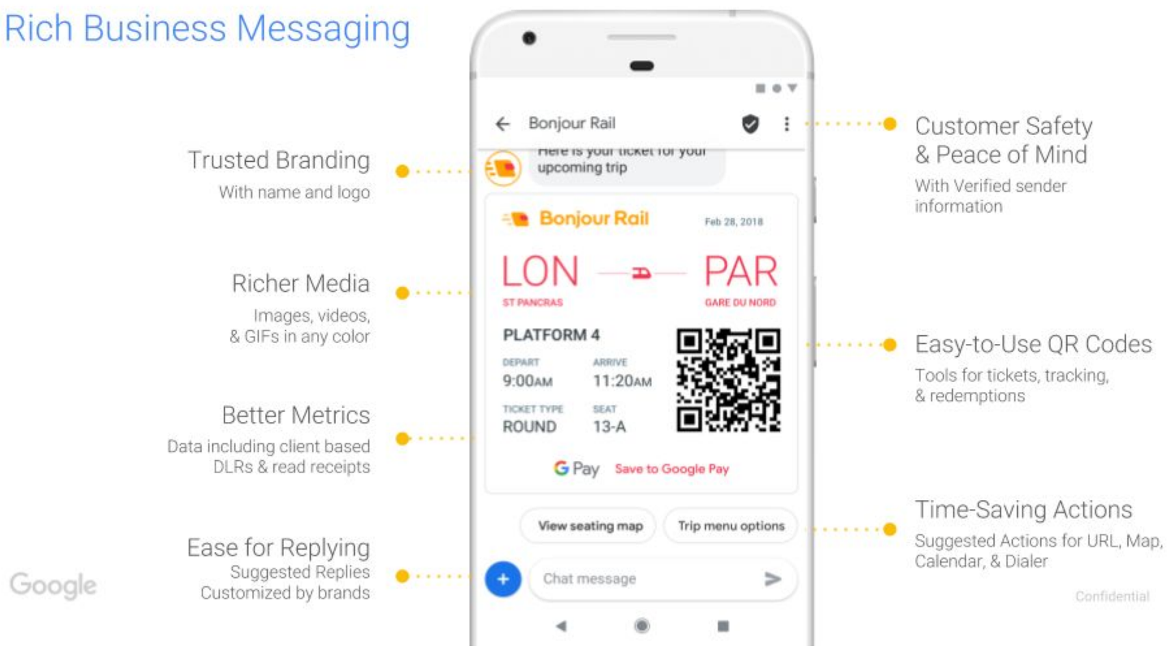
Rich Business Messaging

Q&A relating to data & security

October 2018

Background:

Rich Business Messaging (RBM) is a conversational messaging platform, with which businesses can engage their customers in dialogue relating to transactions, marketing, customer service and other topics. Its is made available through a Google API and delivered to users through their mobile carrier.



Rich Business Messaging

Trusted Branding
With name and logo

Richer Media
Images, videos, & GIFs in any color

Better Metrics
Data including client based DLRs & read receipts

Ease for Replying
Suggested Replies Customized by brands

Customer Safety & Peace of Mind
With Verified sender information

Easy-to-Use QR Codes
Tools for tickets, tracking, & redemptions

Time-Saving Actions
Suggested Actions for URL, Map, Calendar, & Dialer

Typically each business or brand works with a Partner (sms aggregator, bot builder, CS platform, etc) who connects to the Google API and builds or maintains the Agent (the RBM bot or experience) on behalf of the brand.

Each Partner and Agent connecting to the Google API is governed by a standard Terms of Service (ToS) agreement, and (because Google is acting as a Data Processor) a Data Processing and Security Terms (DPST).

Google does not enter into custom or supplementary agreements regarding RBM.

Objectives

The purpose of this document is to provide answers to common questions relating to RBM data security and associated topics.

1. What is the implication that Google is a Data processor?

   Unlike many other Google services, with RBM, Google is positioned as a Data Processor (vs a Data Controller - who would be the business or its bot builder in this instance). The DPST exists to show that we are a data processor, and to govern the terms around us handling the data on behalf of our partners.

2. Does the DPST apply to all the users of my agent?.

   Yes the DPST will apply to all of your users and their data. This is architectural - we've built the platform so all users receive the same high level of data security, and also for compliance.

3. Why won't Google entertain custom agreements for RBM?

   Just like Google Play, our plan for RBM is to scale to a very large number of user experiences, and this requires uniform legal agreements.
   Since we are a data processor we have purposefully designed very partner friendly terms that we believe provide ample protection for businesses and their users.
   We have over 200 brands and 400 agents on the platform today, all using the same ToS and DPST.

4. Our business is subject to regulations that mean that its providers must be available for audit. Will Google co-operate with this?

   We have teams that are dedicated to responding to law enforcement and regulator inquiries in accordance with applicable law.

5. Will Google use my customer's data outside of RBM?

   Google uses customer data only for the purpose of providing and improving the RBM service, as stated in the DPST.

4.2.1 Company's Instructions. By entering into these Terms, Company instructs Jibe to process Company Personal Data only in accordance with applicable law: (a) to provide and improve the Services; (b) as further specified via Company's use of the Services; (c) as documented in the form of the Agreement, including these Terms; and (d) as further documented in any other written instructions given by Company and acknowledged by Jibe as constituting instructions for purposes of these Terms.

6. Is persistent storage used for this service, and where is the information stored (conversations, materials for the agent, etc.)

   MO: Stored on store and forward basis, for not longer than 7 days. As soon as the RBM agent receives/acknowledges the message, it is deleted.
   MT: Typically held for 30 days (or until delivered to the handset) on store and forward basis. Undelivered messages can typically be revoked before delivery by Agent.
   MT: Held encrypted at Google for 14 days, solely for spam detection.
   Agent Materials (logo, name, description, etc): Persistently stored in global Google storage.

7. If a message is not delivered, How would we be notified that the message hasn't been delivered? And what's the mechanism available to us to revoke the delivery of such message(s).

   We report the status of each message. Sent, delivered, read. You can build logic that says (for example), if a message is not delivered within (say) 20 minutes, revoke the message, and send as an SMS.

8. Are such messages stored encrypted?

   Yes - messages are stored encrypted.

9. Can a business control the encryption keys for its messages stored at google?

   Unfortunately not, because Google needs to scan RBM messages for spam to protect all users.

10. Is RBM certified by any 3rd parties?

    RBM and Google's RCS infrastructure are ISO 27001, SOC 2, and SOC 3 certified.
    We expect to be HIPAA certified in Q4 2018. See also this provision in the DPST:

    6.5.1 Reviews of Security Documentation. In addition to the information contained in the

Agreement (including these Terms), Jibe will once these are available provide Company the following documents and information to demonstrate compliance by Jibe with its obligations under these Terms:
1. any certificates issued in relation to the ISO 27001 Certification;
2. the then-current SOC 3 Report (if available); and
3. the then-current SOC 2 Report (if available), following a request by Company in accordance with Section 6.5.3.

11. What audit rights do we have?

    See this section from the DPST:

    6.5.2 Company's Audit Rights.
    1. If the European Data Protection Legislation applies to the processing of Company Personal Data, Jibe will allow Company or an independent auditor appointed by Company to conduct audits (including inspections) to verify Jibe's compliance with its obligations under these Terms in accordance with Section 6.5.3 (Additional Business Terms for Reviews and Audits). Jibe will contribute to such audits as described in Section 6.4 (Security Certifications and Reports) and this Section 6.5 (Reviews and Audits of Compliance).
    2. Company may also conduct an audit to verify Jibe's compliance with its obligations under these Terms by reviewing the Security Documentation (which reflects the outcome of audits conducted by Jibe's Third Party Auditor).

12. How would Google handle data breaches?

    Please refer to the DPST section on Data Incidents:

    6.2 Data Incidents.

    6.2.1 Incident Notification. If Jibe becomes aware of a Data Incident, Jibe will: (a) notify Company of the Data Incident promptly and without undue delay after becoming aware of the Data Incident; and (b) promptly take reasonable steps to minimize harm and secure Company Personal Data.

    6.2.2 Details of Data Incident. Notifications made pursuant to this section will describe, to the extent possible, details of the Data Incident, including steps taken to mitigate the potential risks and steps Jibe recommends Company take to address the Data Incident.

    6.2.3 Delivery of Notification. Notification(s) of any Data Incident(s) will be delivered to the Notification Email Address or, at Jibe's discretion, by direct communication (for example, by phone call or an in-person meeting). Company is solely responsible for ensuring that the Notification Email Address is current and valid.

6.2.4 No Assessment of Company Personal Data by Jibe. Jibe will not assess the contents of Company Personal Data in order to identify information subject to any specific legal requirements. Company is solely responsible for complying with incident notification laws applicable to Company and fulfilling any third party notification obligations related to any Data Incident(s).

6.2.5 No Acknowledgement of Fault by Jibe. Jibe's notification of or response to a Data Incident under this Section 6.2 (Data Incidents) will not be construed as an acknowledgement by Jibe of any fault or liability with respect to the Data Incident.

13. What does the customer see when the RBM service is unavailable?

    When data connectivity is lost: a temporary status bar indicating “No connection”.

    When RCS connectivity is lost (e.g. because the user switched carrier): a persistent status bar indicating that this service is not available, with a link to a help center page about how to regain RCS connectivity.

14. How does Google maintain the security of the Android Messages (app) to MSISDN verification, after the initial silent SMS verification?

    INITIAL VERIFICATION
    Google’s high level goal is to be as secure (or more secure) as SMS
    Typically, initial verification is through “header enrichment” (see RCS spec). Requires custom integration with the carrier. When the RCS client (Android messages) makes a request to enable RCS, Google receives, over cellular data, a packet (header) including MSISDN. Google uses this to send an (invisible) SMS to the RCS client to validate the user and complete the handshake. If for some reason the verified connection is lost (user changes SIM cards, carrier reports that the number is re-allocated, etc), then we repeat the verification process.

    MAINTAINING SECURITY AFTER VERIFICATION:
    The phone number verification handshake ends with a password being sent to the RCS client and stored securely by the app. This password is then used to establish a persistent TLS connection with the RCS backend. This mechanism is part of the publicly available RCS specification, which can be downloaded here.

15. What reporting does Google see on RBM agents?

    Google has internal reporting the gross number of users, messages and responses for each agent, based only on the last 14 days data. We use this for diagnostics and system improvements.

16. Do Section 3.4 (d) through (f) of the Terms of Service limit a brands ability to collect and use information about their customers?

These clauses are not intended to restrict a businesses ability to serve their customers but are to ensure user security and privacy. See below for more details.

3.4 Prohibited Actions. In connection with RCS Business Messaging, you will not, and will not authorize any third party to: (d) collect or use personal and confidential information, such as national identification number or social security number, payment and financial data (e.g., credit card and bank account numbers), log-in credentials, passwords, or answers to security questions;

This is provided to protect users from security risks by sharing personally sensitive information. Message history is stored within the user's messaging app - so another person accessing the phone at some point in the future could potentially look at message history and be exposed to such personal data.

We plan to offer features in the future that will help users transfer sensitive information—e.g. SSNs, credit card numbers—to businesses in a safe and secure manner. For instance, special webviews or other message types specifically for gathering this type of info.

(e) use any information about user's online or offline state for any reason except to directly provide the services to the user, and under no circumstances in a manner that may surprise or disturb a user (including, but not limited to, sending a promotion or advertisement based on them coming back online);

The Capability Check feature is provided to allow Businesses to choose the correct channel to message a business - not to build a profile of offline vs online status for a user, or to provide a trigger to deliver a message based on a change of online status for a particular user.

or
(f) use or share user data without specific user consent for the specific use of that data.

We expect all businesses using RBM to supply a privacy policy and offer guarantees that they will not use/share user data without specific user permission.

Do Google RCS servers store any end user personal data or brand's agent personal data? If yes, is it stored encrypted?
Do Google RCS servers store conversation text? If yes, is it stored encrypted?
"MO: Stored on store and forward basis, for not longer than 7 days" Is this data stored encrypted or in clear text?
Is MT stored for 14 or 30 days? And is it stored encrypted or in clear text?
"Google has internal reporting the gross number of users, messages and responses for each agent, based only on the last 14 days data. We use this for diagnostics and system improvements". Are transcripts stored for 14 days? Or only aggregate information on messaging volume? If transcripts, are they stored encrypted?
How do Google servers and the Google app handle PCI data (credit cards, etc.)?
According to the RBM Q&A doc, "This is provided to protect users from security risks by sharing personally sensitive information. Message history is stored within the user's messaging app - so another person accessing the phone at some point in the future could potentially look at message history and be exposed to such personal data. We plan to offer features in the future that will help users transfer sensitive information—e.g. SSNs, credit card numbers—to businesses in a safe and secure manner. For instance, special webviews or other message types specifically for gathering this type of info". 1. Does this mean that data is stored in clear text on the mobile device? 2. Does this mean that PCI data is not masked and stored in clear text on the mobile device? 3. Is PCI data masked on Google servers?
Does Google RCS support GDPR (the right to be forgotten) , and provide the ability to remove all information stored about a user?
Does Google RCS support the option to prevent backup of conversations from the device to Google Drive?
What authentication mechanism is used between LE connector and Google RCS servers (both ways)?
Does Google RCS support consumer authentication?
Does Google RCS support media sharing? If yes, does it validate the shared content for potential malicious code?
How Google RCS implement data segregation between the different brands?
For data in transit, please provide more insight on the TLS algorithms and key sizes being used for communication with GRBM servers.
Regarding carrier access to RBM data, please provide us with a list of Jibe vs non-Jibe carriers.
Please provide specifics surrounding type of encryption used for both data in transit and at rest.