Data Security in HappyOrNot Service

This document provides an overview to data security in HappyOrNot Service.

Document status

Owner of this security activity: Davide D'Incau

Version (Current version first)	Author	Status	Approved by/Date
1.4	Lauri Fjällström	Approved	29.11.2018 Added details about Smiley Touches and Web Smileys Updated details to match current status
1.3	Davide D'Incau	Approved	22.1.2018 Improved explanation of user account profiles access right specs. Added LTE as one connection network type (Smiley Touch)
1.2	Davide D'Incau	Approved	Updated HON street address. Added security classification.
1.1		Approved	28.4.2016 by Lauri Fjällström
1.1	Lauri Fjällström	Draft	Added CDMA
1.0		Approved	29.9.2015 by Lauri Fjällström
0.2	Davide D'Incau	Draft	Edited text to clarify some of the elements. Ready for approval.
0.1	Suvi Lehtinen	Draft	N/A

About HappyOrNot Service

HappyOrNot enables organizations to collect and analyze anonymous customer and/or employee feedback so to improve satisfaction.

Feedbacks are collected using Smiley Terminals, Smiley Touches and Web Smileys. The collected feedbacks are analyzed in HappyOrNot Reporting Service.

HappyOrNot Smiley Terminals have four smiley buttons users can press to give feedback. The buttons indicate feeling: very satisfied, satisfied, slightly dissatisfied and very dissatisfied. Customers and/or employees can effortlessly give feedback about their service experience by pressing one of the buttons on the feedback interface. The system records at every button press the value (green, light green, light red, red) and the associated time stamp.

In addition to the four smiley buttons, Smiley Touches have option to send follow-up options and open feedbacks to give the reason behind the feeling. Web Smileys have the open feedback option in addition to the smiley buttons.

Neither Smiley Terminals, Smiley Touches nor Web Smileys record any information that can be used to identify or track individuals.

The feedback data is sent either periodically or in real-time to be processed in HappyOrNot Reporting Service. Results are distributed in the form of satisfaction reports to the respective customers via a web application (https://reporting.happy-or-not.com), email or REST API.

Confidentiality

Confidentiality in Data Transmission

HappyOrNot Smiley Terminals and Smiley Touches use 2G/3G/CDMA/LTE mobile networks to send feedback data to the HappyOrNot Service. The feedback data is sent using either SMS messages or mobile data. Confidentiality of 2G/3G/CDMA/LTE networks is included in the respective network standards and Mobile Network Operators are responsible for implementing and maintaining them in their networks. Mobile Network Operators forward the feedback data through encrypted VPN connections to HappyOrNot Service.

Smiley Terminals and Smiley Touches that have mobile subscriptions aimed for consumers are exceptions. Smiley terminals deployed before 2014 and early Smiley Touch revisions shipped in late 2017 belong to this group that don't utilize the encrypted VPN connections in their data transmission. These Smiley Terminals use external SMS gateways or direct TCP connections to HappyOrNot Service to send the feedback data. SMS gateways use encrypted HTTPS connections but direct TCP connections are unencrypted. All Smiley Touches use encrypted HTTPS connections. There are currently less than 1000 such Smiley Terminals and Smiley Touches in total.

Neither Smiley Terminals nor Smiley Touches require any infrastructure from the clients nor do they integrate in any way to clients' infrastructure.

HappyOrNot Web Smileys use encrypted HTTPS connections for all data transmission.

Confidentiality in HappyOrNot Reporting Service

HappyOrNot users have two ways to access the feedback data in HappyOrNot Service. They can log into HappyOrNot Reporting Service or they can subscribe to email reports in HappyOrNot Reporting Service to get the results via email. HappyOrNot Reporting service is accessed using encrypted HTTPS connections. Email reports use standard SMTP delivery and thus their transmission is not encrypted. Email report contents are an aggregated subset of the clients feedback data typically including the results for a specific period of time (day, week, month).

HappyOrNot clients can also retrieve programmatically the results and store/integrate them into their systems using the HappyOrNot API. The API is used through TLS encrypted HTTPS connections.

Each client and its users can only access data of their own organization. Users must authenticate using their own personal credentials to the HappyOrNot service. HappyOrNot authentication is based on user id (email address) and password. Password are stored in salted hashed form. The API can be accessed using a client id and an application API token generated by HappyOrNot Reporting Service. The API access is disabled by default.

Access control is a combination of role based access control and responsibility based access control. User's role defines what the user can do in the system. User's responsibilities define what data the user is able to access. User's responsibilities will usually be derived from organizational hierarchy and associated responsibilities.

The roles in HappyOrNot Reporting Service are:

1. **Happy User**: Happy user role is only granted to HappyOrNot employees who have valid written employment/collaboration contract with HappyOrNot. The contract includes a NDA (Non Disclosure Agreement). These users have **read access to all the feedback data** available in HappyOrNot Reporting Service **and read/write access to settings** data (company, users, surveys, terminals settings).
2. **HappyOrNot Partner**: granted to employees of official HappyOrNot resellers with valid reseller agreement. Partner role has **read access to feedback data** and **read/write access to settings data** of their direct clients. Partners must comply to HappyOrNot partner agreement and are also bound to their agreement with their customers. Such agreements include NDA. HappyOrNot resellers manage their user accounts internally and create user accounts to HappyOrNot Service on need basis.
3. **Client Admin**: have **read access to the feedback data** collected in their organization and **read/write access to the settings data** of their own company. They can manage user accounts of their own company. The user role only have read access to their own company's data.
4. **User**: **only have read access** to their own company's feedback data.

Important: None of the users types have rights to change the feedback (counts or feedback type) collected by HappyOrNot Smiley Terminals and stored in HappyOrNot Service.

With responsibility based access control it is possible to further limit what data partner, administrator and user roles can access. As an example, the access can be limited to certain subsets of the organizational branches (e.g. one store/location, one region, one sub-organization/team).

Physically all the data from different HappyOrNot clients is stored in the same database. Access control to the data is handled in application code according to user role and responsibilities. In the application architecture the business logic is separated from other layers and the business logic is responsible for doing appropriate authorization checks.

Confidentiality in HappyOrNot Server Infrastructure

HappyOrNot servers and databases are located in Amazon Web Services (AWS). All the servers needed by HappyOrNot Service are in EU (Ireland) inside a virtual private cloud. Access to the servers must be made through encrypted VPN. Access to the VPN is granted to HappyOrNot technical employees only. The authentication process for the VPN is single factor authentication that uses public key cryptography.

As all the data stored in HappyOrNot Service is nonsensitive and the feedback data is anonymous, all disks, databases and backups are not encrypted.

Integrity

Integrity of data in transit

Data coming from Smiley terminals includes checksums. Integrity of data received over HTTPS from reporting service is provided by TLS protocol.

Integrity of data in rest

HappyOrNot database is a transactional database. No other means are utilized to ensure the data integrity.

Integrity of HappyOrNot Server Infrastructure

Please refer to our *Host and network security basics activity*.

Availability

HappyOrNot service had been built on a service oriented architecture to make it fault tolerant and scalable. Critical services have been built redundant to ensure high availability.

HappyOrNot database supports point-in-time recoveries and a full snapshot is taken every day. The retention period for the daily snapshots is 35 days. The snapshots can be accessed by HappyOrNot technical employees who have access to the HappyOrNot private virtual cloud.