Furhat Robotics
Platform Data Security & Privacy Overview

Product Description

Version 1.2

Contents

Introduction

This document is intended to describe the data security & privacy characteristics of the Furhat Platform from a customer perspective. It covers the following topics:

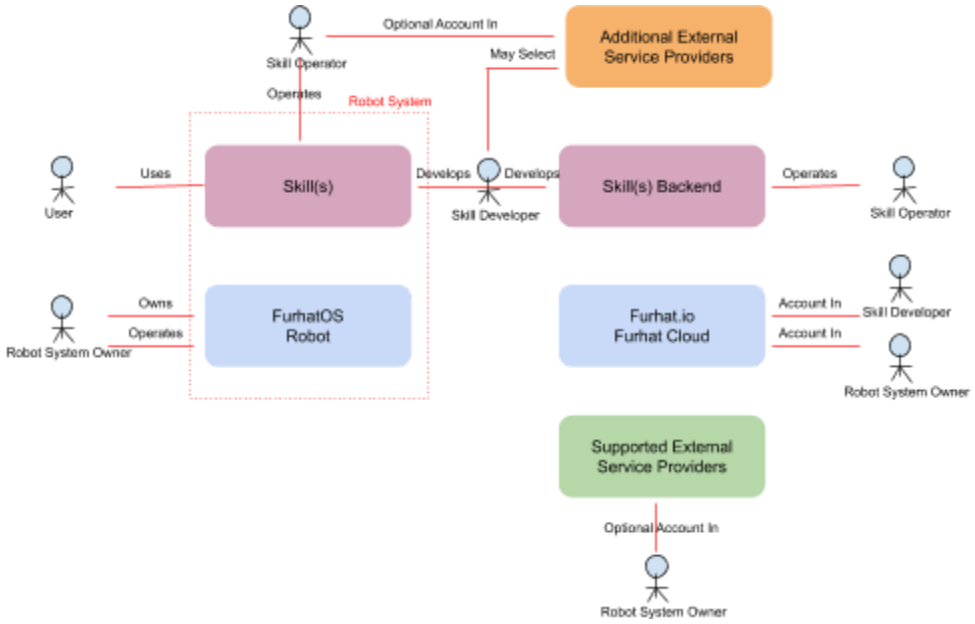
- Entities & Layers
- Identities & Accounts
- Speech Data
- Vision Data
- System Data
- External Service Providers
- Remote Operations & Maintenance (O&M)
- General Data Protection Regulation (GDPR)
- Frequently Asked Questions (FAQ)

The contents of this document are subject to continuous improvement and revision, in line with the evolution of Furhat products and *Supported External Service Provider* offerings.

Entities & Layers

This chapter introduces the Entities and Layers necessary to define and communicate data security & privacy concerns and solutions within the product.

Key Entities



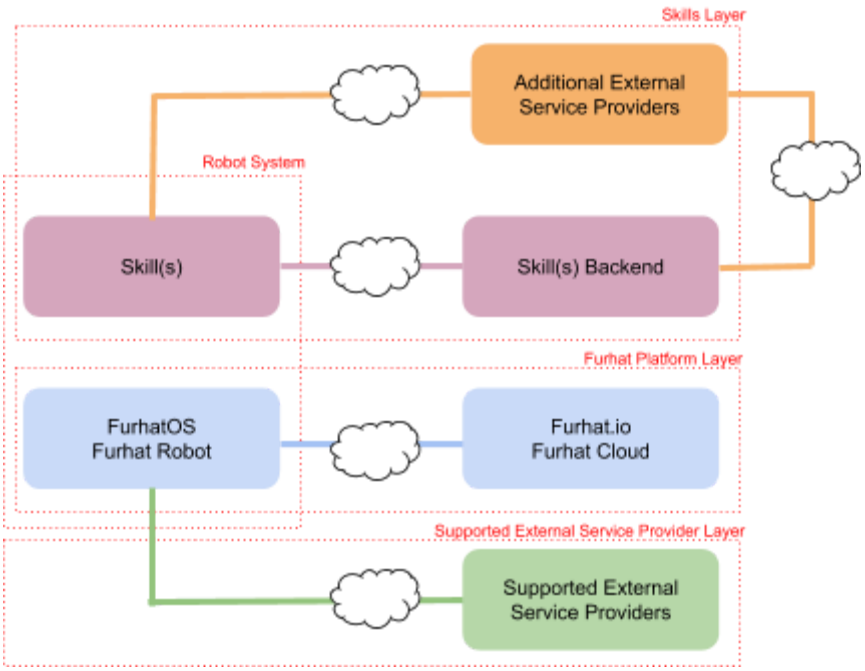
Entity	Description
Robot	Refers to a Furhat Robot pre-loaded with a standard FurhatOS installation
Robot System	Refers to a *Robot*, running one or more *Skills*, and deployed by a *Robot System Owner* in order to fulfill a certain set of tasks within the *Robot System Owners* business
Robot System Owner	Refers to the owner, and generally operator, of a *Robot System*.
User	Refers to people who interact with the *Robot System* from the end user perspective, i.e. users interact with the services/experience provided by *Skills* running on the *Robot System*.

Skill	Refers to an application that runs on a *Robot* and delivers services/experience to *Users*. A *Skill* is comprised of a skill software package that is installed onto, and runs on the *Robot*. A *Skill* will also frequently have a *Skill Backend*, that will generally run on a public, private, or hybrid cloud setup
Skill Developer	Refers to the organisation that has developed the *Skill* code and provides the skill software package to a *Robot System Owner*. The *Skill Developer* generally also provides technical support and updates to the skill over time.
Skill Operator	Refers to the organisation that operates the *Skill*. A *Skill* may have both front and back end (i.e. cloud) based components, and the operation of the skill may require data processing, retention, management, and other tasks within the *Skill Operator*'s cloud.
Furhat Platform	Refers to *FurhatOS*, *Furhat.io* (Furhat's site for developers) and *Furhat Cloud* (Furhat's general cloud and backend systems)
FurhatOS	Refers to Furhat's proprietary operating system, the system software that runs on every *Furhat Robot*, and the host for all *Skills*
Supported External Service Provider	Refers to external service providers which the *Furhat Platform* provides built-in support for. Current examples are *Google ASR*, *Amazon Polly*, *Microsoft Azure Cognitive Services ASR*, *Amazon S3* etc.
Additional External Service Provider	Refers to external service providers which a *Skill Developer* or *Skill Operator* uses as part of their skill architecture and implementation.
Identity	Refers to data that uniquely identifies entities such as a *Robot*, *User*, *Robot System Owner*, *Skill Developer*, *Skill Operator*, *Supported External Service Provider* etc.
Credential	Refers to a secret, generally used together with an *Identity* in order to facilitate authentication, authorisation, and other security functions.
Account	Refers to an entity that reflects the presence of a *Robot User*, *Robot System Owner*, *Skill Developer*, *Skill Operator* etc. within a system. Accounts generally include *Identities*, *Credentials* and other business/system data related to the entity.

Key Layers

This chapter places the entities (see above) in context and introduces key principles for sets of entities grouped in the key layers *Platform*, *Skills*, and *External Service Provider*.

In general, diverse types of data (e.g. identities, accounts, speech, video) are processed on different layers, and different parties are responsible for the design, operation and compliance of data security & privacy in those layers



Platform Layer

The *Platform Layer* refers to the *Furhat Robot*, *FurhatOS*, *Furhat.io* (Furhat Robotics' site for developers) and *Furhat Cloud* (Furhat's general cloud and backend systems). These are entities which Furhat Robotics has design, engineering and operating responsibility as well as control.

Principles
Furhat Robotics is responsible for ensuring data security, privacy and regulatory compliance, for data that is processed by any, and all, components of the *Platform Layer*.
Furhat Robotics is responsible for configuring, managing, and documenting the interfaces between the *Platform Layer* and *Supported External Service Providers* (e.g. speech recognition, speech synthesis, cloud databases etc.)

Furhat Robotics is also responsible for ensuring that the design and implementation of interfaces within the *Platform Layer* adhere to industry best practices for security (e.g. authentication, authorisation, encryption etc.)
Robot Owners/*Skill Developers*/*Skill Operators* may elect to configure their own accounts for *Supported External Providers* within the *Platform Layer*, thereby taking control over the management of those accounts and having the freedom to tailor those account configurations to their own specific security preferences and policies over time.

Skills Layer

The *Skills Layer* refers to *Skills code* (deployed to a Robot), *Skills Backend* (that serves or provides network or cloud based services to the Skills code) and any *Additional External Service Providers* which the skills architecture and implementation relies upon and interacts with.

Principles
The *Skill Developer*/*Operator* is responsible for ensuring security, privacy and regulatory compliance, for data that is processed by any and all components of the *Skills Layer.*
The *Skill Developer*/*Operator* may include *Additional External Service Providers* as part of their skill architecture/implementation. In such cases, the *Skill Developer*/*Operator* is responsible for ensuring security, privacy and regulatory compliance, for data that is processed by any and all such *Additional External Service Providers.*
The *Skill Developer*/*Operator* should maintain a data security and privacy specification for their *Skill* and make this available to *Robot System Owners*
In cases where the *Robot System Owner* is distinct from the *Skill Developer*/*Operator* the *Robot System Owner* is responsible for ensuring data security, privacy and regulatory compliance for data that is processed by their *Robot System*

Supported External Service Provider Layer

The Supported *External Service Provider Layer* refers to external service providers (e.g. Speech Recognition, Speech Synthesis etc.) for which the *Furhat Platform* has built-in support.

Principles
Furhat Robotics is responsible for configuring, managing, and documenting the interfaces

between the *Platform Layer* and *Supported External Service Providers* (e.g. speech recognition, speech synthesis, cloud databases etc.)
Furhat Robotics is responsible for ensuring that the design and implementation of interfaces towards *Supported External Service Providers* within the *Platform Layer* adhere to industry best practices for security (e.g. authentication, authorisation, encryption etc.)
Furhat Robotics is responsible for understanding the data security and privacy aspects of the *Supported External Service Providers* and communicating the details of these with *Skill Developers/Operators* and *Robot System Owners*

Identities & Accounts

This chapter deals with the topics of *Identities* and *Accounts* within the overall system from a security and privacy perspective.

Platform Layer

The following table relates to *Identities* and *Accounts* managed within the *Platform Layer*.

As a general principle it should be noted that the identities and accounts within the platform layer serve the *technical* and *business level* interactions between Furhat Robotics and related *Robot System Owners*, *Skill Developers*, *Skill Operators,* and *Supported External Service Providers*. *Platform Layer* identities and accounts do not relate to the (end) *User*.

Identity	**Description**	**Security / Privacy**
Robot Identity	Each Robot has a unique identity of the form `Furhat-<Number>`, which is presented, at the top of the on-face menu. The *Robot Identity* can be used to address network traffic to the Robot on the local network to which the Robot is connected. (`Robot Identity = hostname`)	The *Robot Identity* is used in over the network communications between the *Robot* and Furhat Robotics business systems. These communications currently use HTTP[1].
Robot Admin Identity	Each Robot has a credential which is required in order to access the Robots web-console.	This credential can be changed by the *Robot System Owner* and it is recommended that the credential be changed from it's default setting.
Robot System Owner Identity	Reserved for future use	Reserved for future use
Google ASR Identity & Credential	Each *Robot* may store an identity and credential used to access Google ASR capabilities. The identity/credential pair may be	The respective identity and credential can only be changed via the web-console after authentication using a valid Robot admin credential

[1] Roadmap: It is planned to convert these to HTTPS/TLS

	provided via Furhat Robotics systems OR may be configured separately by the *Robot System Owner.* The actual account containing additional system, business and personal data relating to the use of Google ASR is held within Google Cloud Platform (GCP) systems.	
Amazon Polly Identity & Credential	Each Robot may store an identity and credential used to access Amazon Polly TTS capabilities. The identity/credential pair may be provided via Furhat Robotics systems OR may be configured separately by the *Robot System Owner.* The actual account containing additional system, business and personal data relating to the use of TTS is held within Amazon Web Services (AWS) systems.	The respective identity and credential can only be changed via the web-console after successful authentication using a valid Robot Admin credential.
Acapela Cloud[2] Identity & Credential	Reserved for future use	Reserved for future use
Amazon S3 Identity & Credential	This identity and credential is used for dialog logging. The actual account containing additional system, business and personal data relating to the use of S3 is held within Amazon Web Services (AWS) systems.	The actual identity and credential are associated with a Skill Developer account in Furhat.io and are fetched from Furhat.io using the respective Skill Developer token.
Skill Developer Identity	Each *Skill Developer* has a unique identity and credential assigned to them on registration at Furhat.io Each *Robot Skill Developer* has an account within Furhat.io. The account contains additional system,	The developer identity and credential are stored on Furhat.io. The credential is encrypted. The Skill Developer, once logged in to Furhat.io can

[2] Roadmap: Support for Acapela Cloud voices is planned for a coming platform release.

	business and personal data relating to the Robot Skill Developer.	change their credential, name, and view their API token.
Skill Identity	Reserved for future use	Reserved for future use
Skill Operator Identity	Reserved for future use	Reserved for future use

Skills Layer

Identities and *Accounts* within the *Skills Layer* are generally defined, managed and fully within the control of the *Skill Developer* and *Skill Operator*.

Skills also have potential to get involved with the identities of end *Users*. Handling the identities and managing accounts representing end *Users* will place a set of requirements[3] on *Skills Developers/Operators*.

Skill Developers/Operators should apply security best practices and principles in the design, management and operation of identities and accounts within their respective skill architectures and implementations. They should also be aware of, and comply with all applicable local and international data security & privacy regulations.

Supported External Service Provider Layer

When *Platform Layer* built-in identities and credentials are used to interact with *Supported External Service Providers,* then these are associated with Furhat Robotics accounts at the respective service providers *Google*, *Amazon* and *Acapela*.

Robot System Owners are free to set up their own identities and accounts at the respective service providers and also configure the necessary identities and credentials on their *Robot Systems* so that Furhat Robotics accounts are no longer used. In such cases, *Robot System Owners* are responsible for the secure handling and configuration of the respective identities, credentials and accounts.

[3] Similar to those faced by any modern App Developer/Operator, but with additional attention to video/speech/image/dialog data.

Additional External Service Provider Layer

Additional External Service Providers are service providers selected by *Skill Developers/Operators* in order to support their specific skills, and do not have built-in support in the *Platform Layer*.

Identities and *Accounts* within the *Additional External Service Provider Layer* are always defined, managed and fully within the control of the *Skill Developer*/*Operator*.

Skill Developers/*Operators* should apply security best practices and principles in the design, management and operation of identities and accounts within their respective Skill architecture and implementation. They should also assess any selected *Additional External Service Providers* from the perspective of all applicable local and international data security & privacy regulations.

Speech Data

Robot Systems are capable of both synthesizing and recognizing speech. The system supports multiple different flavours of speech synthesis, and understanding, depending on system installation (e.g. installed voices) and configuration (e.g. online/offline synthesis, service provider selection etc.)

Dialog Data

Speech has a natural relationship with the contents of dialogs[4], which are in turn generated by *Skills*. *Skills* receive speech data in the form of dialog `text`; similarly Skills generate dialog content in the form of `text`. *Platform Layer* capabilities can then synthesize speech from `text` and also generate `text` from audio streams using speech recognition features.

Principles
Skill Developers/Operators have extensive access to dialog data in the form of text. This dialog data contains both dialog generated by the skill itself, but also data received from speech recognition. Such data will contain extensive information from speech that has been detected by the *Robot System*, this information may contain private, personal and business sensitive information and must be handled securely and in compliance with all required legislation. Significant attention should be paid to *informing users that data is being recorded*, *if and how dialog data is to be retained*, *how it is stored*, *who has access to the data* etc.
The *Platform Layer* does not store dialog data unless a *Skill Developer* has explicitly activated dialog logging within their skill. This is generally done to support skill development, debugging, and improvement and is switched off by default. If Dialog logging is enabled, the logs are stored locally on the Robot at `/home/furnix/logs`. If the *Skill Developer* has also supplied a developer token when enabling logging, all data will also be stored in a Furhat Robotics managed Amazon S3 storage bucket, This enables the developer to view and also manage their dialog logs using the Cloud Dialog viewer tool on Furhat.io. If requested this logging destination can be changed to a *Skill Developer* managed Amazon S3 storage bucket.

[4] The conversation between Robot Systems and Users

Raw Audio

Audio input and output streams are supported by the *Robot* microphones and speakers respectively. Some of the audio input will contain speech input[5], whereas most of the audio output is speech output from skills running on the *Robot*.

Principles
Raw audio data is only available within the *Platform Layer* and is not[6] exposed to the *Skills Layer*.
Raw audio data is only logged when a *Skill Developer* has explicitly activated dialog logging within their skill. Dialog logging is switched off by default (see dialog data above).
Raw audio data is passed to a *Supported External Service Provider* (e.g. *Google ASR, Microsoft Azure Cognitive Services ASR*) for the purposes of speech recognition (see speech recognition below).

Speech Recognition

Speech Recognition relates to the process whereby audio data containing speech is converted into `text` representing the speech contents by the system.

Principles
Cloud based speech recognition services are used due to the superior quality of performance & accuracy (compared to offline STT). The *Platform Layer* includes built-in support for *Google ASR*[7] and *Microsoft Azure Cognitive Services ASR* as *Supported External Service Providers*. By default *Google ASR* does not retain any logs of audio data or resulting recognized text, but can be configured (opt-in) to retain audio and recognizer logs. Google accounts managed by Furhat Robotics for the provision of built-in support of ASR in the platform layer use the default setting which is no logging of audio data or recognized text. Please see the relevant Google SLA and policy for details https://cloud.google.com/speech-to-text/docs/data-logging By default *Microsoft Azure Cognitive Services ASR* does not log raw audio data or the resulting transcribed text. Please see the relevant Microsoft SLA and policy for details https://azure.microsoft.com/en-us/services/cognitive-services/speech-to-text/#security Audio data in transit from a Robot System to Google ASR and Microsoft Azure Cognitive Services ASR TLS in order to achieve on the wire security.

[5] Other ambient noise will also be present in the audio input.

[6] Some developer customers have requested the ability to receive raw audio data from the Platform Layer

[7] Google Cloud Speech-to-Text

As previously noted, a *Robot System Owner* can configure their own Google or Microsoft Azure account including enabling the use of ASR and opt-in (where available) to the retention of audio and recognizer logs on supported external service providers if they so wish. Robot System owners should exercise due care that the activation of audio and recognizer logs on their own accounts complies with security best practices and applicable regulations.

Speech Synthesis

Speech Synthesis relates to the process whereby `text` data is converted into human-like speech, in a selected synthetic voice, by the system.

The *Platform Layer* supports both cloud based (e.g. *Amazon Polly*) and offline (e.g. *Acapela* or *Cereproc*) based speech synthesis and this is determined by which synthetic voice has been selected in the Robot System; different security and privacy principles are relevant depending on whether cloud based or offline speech synthesis is used.

Principles
Offline Speech Synthesis (e.g. Cereproc or (non-cloud) Acapela voices)
In Offline Speech Synthesis, dialog data generated by the *Skills Layer* results in speech being generated by offline synthesizers resident on the *Robot System*. As no *External Service Provider* is involved, Dialog data does not leave the *Robot System* (unless dialog logging is activated) and the resulting speech data is only available within the *Robot System*.
Audio (`.wav`) and phonetics (`.pho`) files generated as a result of speech synthesizers are cached on the Robot in order to improve the performance of subsequent synthesizer requests for the same dialog data. The cached data is stored at `/home/furnix/Synthesizer`[8]. The clear cache feature on the web-console can be used to delete the cached speech data at any time.
Cloud Based Speech Synthesis (e.g. Amazon Polly, Acapela Cloud voices)
In Cloud Based Speech Synthesis, dialog data generated by the Skills Layer results in text being sent to a cloud based text to speech service which returns audio in a specified synthetic voice. By default Amazon Polly does retain and use text and resulting speech for the purposes of improving the quality of both Polly and other machine learning based services at Amazon, it is possible to explicitly opt-out of this retention and usage. Amazon accounts managed by Furhat Robotics for the provision of built-in support of speech synthesis in the platform layer are set to opt-out[9]. Dialog data and speech audio in transit between a Robot System and Amazon Polly uses

[8] Roadmap: Additional measures will be taken to protect cache files, e.g. full disk encryption, periodic automated cache purge etc.

[9] Roadmap: Furhat should re-verify that this opt-out setting has been fully effected on Amazon Polly

TLS in order to achieve on wire security.

Please see the relevant Amazon Polly SLA and policy for further details on Polly data privacy https://aws.amazon.com/compliance/data-privacy-faq/

Vision Data

Robot Systems are capable of visually perceiving the space in front of them using the *Robot's* onboard camera system. This capability is used to detect the presence of *Users* and to track the *Users* for the purposes of developing a situation model (see below) which can be used by *Skills*.

Raw Video

Principles
Raw Video data is only available to the *Platform Layer* and is not[10] exposed to the Skills Layer.
Video is not logged on the Robot and there is no video logging feature in the system currently.
A Video stream which is overlaid with situation model markers[11] is available in the Robot's web-console to *Robot System Owners* who have successfully authenticated with the *Robot.* The Video stream between the Robot and the Robot's Web-Console uses WebRTC[12] for streaming. On robots configured as type `Research`, and where the robot operator has explicitly enabled the Camera Feed feature in the robots Web-Console, a raw video feed will be exposed on the local network using a `ZeroMQ` transport. Due consideration for all applicable ethical and regulatory requirements should be given when enabling the camera feed.

Situation Modelling

The *Platform Layer* generates a situation model using the data perceived from camera video. This situation model detects the presence of users, and tracks the users as they move across the Robots frame of view. The situation model is used to enable higher level capabilities such as attention, gaze direction, user management, and is also available to the Skills Layer.

Principles
The situation model is purely abstract and no connection with real Users, their identities, or

[10] Some Skill Developers have requested the ability to receive raw video data from the Platform Layer

[11] For example bounding boxes around detected faces.

[12] Roadmap: Encryption will be added to the WebRTC streams

Video/Still image or Audio data exists.

System Logs

Robot Systems log data relating to the internal lower level operations and state of the system on a continuous basis. The *Platform Layer* components such as those dealing with *audio*, *video*, *motion control* etc. all perform low level logging and logs are processed using the standard `systemd` features available in the host OS Linux. The contents of the logs are only meaningful to engineers with internal knowledge of the overall system and are only useful for troubleshooting activities.

Platform Layer

Principles
Platform Layer components[13] send low level logs to standard log destination `/var/log`. These logs are persisted and logs are rotated periodically.
Platform Layer components do not log sensitive data such as *audio*, *video*, *dialog*, *identities*, *credentials*, *IP addresses* etc. as part of their system logging features.

Skills Layer

Principles
Skills are developed in Kotlin and a Skills Developer could elect to implement lightweight or comprehensive skills logging within their skill code. Since the Skill has full knowledge of the dialog contents, it is also possible that a Skills own logs could contain sensitive information from dialogs. Skills Developers/Operators should apply security best practices and principles in the design, management and operation of any skills logs within their respective skill architecture and implementation.

[13] For example: *servocore*, *audiocore*, *camcore*, *arduinocore* etc.

Remote Operations & Maintenance (O&M)

Robot Systems enable *Robot System Owners* to authorize remote personnel to access the Robot System and both view and change the installation, configuration and state of the Robot System. Remote personnel can conduct maintenance, troubleshooting or monitoring of the system on request of the *Robot System Owner*.

Remote Support Access

Principles
The *Robot System* is configured to enable authorized remote personnel access via secure shell (SSH). This requires the *Robot System Owner* to engage *remote support mode* via the Robots web-console which in turn enables the robot to tunnel out to the Furhat Support Proxy which in turn bridges a connection to a remote support technician at Furhat Robotics.
The *remote support mode* grants authorized remote personnel powerful[14] access to the Robot System, and due care should be exercised in the activation of remote support mode.

System Telemetry

Principles
The *Robot System* has a telemetry feature that enables it to send basic system level data over the network to Furhat Cloud on a periodic basis. This data can be used by Furhat support personnel to expedite the handling of support cases from *Robot System Owners.*
As of software version 1.12.0, the telemetry data covers the following data: `robot identity`, `machine identity`, `platform software version`, `CPU temperature`, `HDD temperature`.

[14] Root user level access enabling installation/removal of software, viewing of system data, transferring data to/from the robot etc.

General Data Protection Regulation (GDPR)

The GDPR, effective from May 2018, replaces the *1995 EU Data Protection Directive*. The GDPR stipulates requirements for businesses and organizations operating in Europe and/or serving users in Europe. GDPR:

- Regulates how businesses/organisations can *collect*, *use*, and *store* personal data
- Builds upon current documentation and reporting requirements to increase accountability
- Authorizes sanctions on businesses/organisations who fail to meet its requirements

Furhat Robotics Commitment To GDPR

Furhat Robotics is committed to the security and privacy of user and customer data.

Principles
We commit, in all relevant commercial contracts, to comply with GDPR, in relation to the processing of personal information relating to *Robot System Owners*, *Skills Developers*, *Skills Operators*, and all other types of customer and partner data processed by the *Platform*.
We provide documentation that helps *Robot System Owners*, *Skills Developers* and *Skills Operators* better assess the *platform* from a privacy perspective
Where relevant, we will provide specific *platform* features[15] in order to help protect personal data, and achieve regulatory compliance.
We commit to continuously improve the *platform,* as GDPR and other applicable regulations and standards change over time

Data Protection Commitments

Furhat Robotics is committed to our data processing agreements, processing according to instructions, and processing with appropriate confidentiality and access control.

Principles

[15] Example: Features to purge internal audio caches on the request of the Robot System Owner via the robot web-console

Data relating to *Robot System Owners*, *Skills Developers*, *Skills Operators*, and all other types of customer and partners will be processed only in accordance with the customer's instructions, as described in the related data processing terms of our standard contracts.
All Furhat Robotics personnel are required to sign a confidentiality agreement, and complete mandatory confidentiality and privacy training, which instructs on responsibilities, and expected behavior, with respect to the security and privacy of customer data
Access to customer data is granted only to specific roles, and these roles only granted to personnel whose job performance explicitly requires access to the relevant data.

Subprocessor Usage

The *Furhat Platform* provides built-in support for specific *Supported External Service Providers* which qualify as subprocessors from a GDPR perspective. It is important that subprocessors have the necessary technical expertise, processes and commitment to data security and privacy.

Principles
Furhat Robotics makes information on the data security and privacy compliance of *Supported External Service Providers*[16] available as part of our product documentation and contractual framework.
Furhat Robotics evaluates prospective *External Service Providers* from a data security and privacy perspective before they are offered as *Supported External Service Providers* with built-in support in the platform.

Data Return & Deletion

The Furhat Platform provides the support for important data return and deletion requirements.

Principles
Skill Developers/Operators will[17] be able to delete their accounts on Furhat.io with the effect that all of their account data will be removed from Furhat.io

[16] See information in relation to current Supported External Service Providers earlier in this document

[17] Roadmap: The delete feature will be available in a future release of the Furhat Platform

Skill Developers/Operators will be able to export[18] their accounts on Furhat.io with the effect that all of their account data is available for their specific internal business or technical uses
Skill Developers can delete dialog logging data from using features in the cloud dialog viewer tool on Furhat.io
Robot System Owners will be able to request the export[19] and deletion of their accounts on Furhat Cloud, should they cease to have a business relationship with Furhat Robotics
Robot System Owners will be able to delete cache data on robot systems using features[20] available on the robot systems web-console

Data Controller Support

The Furhat Platform provides the support for key Data Controller[21] requirements

Principles
Data Controllers at *Robot System Owners* and *Skill Developers/Operators* can use Platform features such as those on the Robot System web-console, Furhat.io and Furhat Cloud in order to maintain their account data within the system. This includes support for Return and Deletion requirements
Furhat Robotics will promptly inform the relevant parties of any incidents relating to their data in line with reporting terms in our standard contracts.

International Data Transfers

Reserved for future use

Standards & Certifications

Furhat Robotics is committed to adopting relevant international standards and certifications in line with the usage growth for the Furhat Platform

[18] Roadmap: The export feature will be available in a future release of the Furhat Platform

[19] Roadmap: The export feature will be available in a future release of the Furhat Platform

[20] A `clear speech cache` feature is available on the web-console under from FurhatOS release 1.16.0 and onwards

[21] Data controllers are responsible for implementing appropriate technical and organisational measures to ensure and demonstrate that any data processing is performed in compliance with the GDPR. Controllers' obligations relate to principles such as lawfulness, fairness and transparency, purpose limitation, data minimisation, and accuracy, as well as fulfilling data subjects' rights with respect to their data.

Principles
The most relevant international standards are: *ISO 27001 - Information Security Management* *ISO 27019 - Cloud Security* *ISO 27018 - Cloud Privacy*

Frequently Asked Questions (FAQ)

Question	Answer
Can external parties remotely access the contents of my robot ?	No, only somebody with appropriate network access, the IP address of your Robot, and the necessary web-console admin credential can access the web-console of your Robot. Network based SSH access to the Robot is only possible if you explicitly activate remote support mode on the robot and a secure session is established to the Furhat remote support proxy.
Can Furhat Robotics access my Robot ?	No, Furhat Robotics personnel can only access your robot if you explicitly activate remote support mode on the robot and a secure session is established to the Furhat remote support proxy. Furhat Robotics will never access your Robot unless expressly requested and instructed by an authorised member of your team.
What information does Furhat Robotics have on my Robot?	Furhat Robotics has provisioning related information such as the version of the platform software installed on your robot at delivery time. Furhat Robotics also knows which voices, faces etc. were installed on your Robot at delivery or software update time. Furhat Robotics receives periodic system level telemetry from your Robot in order to support diagnostics and troubleshooting activities which are conducted solely on your instruction, and only with your express authorisation.
Does Furhat Robotics receive audio, video, dialog, or other sensitive data from my Robot?	No, Furhat Robotics does not receive such data by default. (see also dialog logging)
Do *Skill Developers* or *Skill Operators* receive audio, video, dialog or other sensitive data from my Robot?	*Skill Developers/Operators* can activate dialog logging in their skill for the purposes of troubleshooting and improvement. When dialog logging is activated, and a developer token has been supplied, dialog and audio data will be logged to cloud storage, where it can also be accessed and viewed by the Skill Developer/Operator

	using our cloud logging tools. Generally speaking Dialog logging should not be activated when a Skill is in a production deployment.
Do *Supported External Service providers* receive audio, video, dialog or other sensitive data from my robot?	Yes, *Supported External Service Providers* which the Platform Layer has built-in support for do receive dialog and audio data. Different policies are in place at each of the *Supported External Service Providers* (please see the sections on *Speech Data* and *Vision Data* in this document) .
In a case where my Robot is stolen or lost, is there sensitive data on the Robot?	Yes, there will be audio data remaining in the speech synthesizer caches[22]. The robots speech cache can be cleared using the clear cache feature in the web-console at any time. Furthermore, since the Robot's storage volumes are unencrypted[23] there will also be various forms of other data, such as identities, credentials, skills packages etc. that are vulnerable in the case of theft or physical compromise.

[22] Roadmap: Additional measures will be taken to protect cache files, e.g. full disk encryption, etc.

[23] Roadmap: Future versions of the platform are likely to introduce full disk encryption

Revision History

Revision	Date	Related SW-Versions	Description
1.0	20191016	>= FurhatOS 1.12.0	Declared full revision status on this.
1.1	20200204	>=FurhatOS 1.16.0	Reflected the clear synthesizer cache feature
1.2	20200923	>=FurhatOS 1.22.0	Reflected the presence of Microsoft Azure ASR Reflected the presence of the Camera Feed feature

Glossary

ASR	Automatic Speech Recognition
DPO	Data Protection Officer
FAQ	Frequently Asked Questions
GDPR	General Data Protection Regulation
O&M	Operations & Maintenance
SSH	Secure Shell
STT	Speech To Text
SW	Software
TLS	Transport Layer Security
TTS	Text To Speech