# The Capturi Platform description

- an understanding of the Capturi platform and implemented security measures

# Technology

Capturi is a Danish proprietary software platform. Capturi's customers purchase a license-based subscription for the platform. The Capturi service is therefore a classic web-based "Software as a Service" service.

The platform's core service is analysis of Capturi's customers' recorded customer conversations and e-mail correspondence with customers. Capturi enables customer service managers and team leaders to gain insight into their agent’s conversations with the company’s customers, allowing them to use such insights to drive even better customer service.

Capturi's entire business foundation is based on Capturi's customers being comfortable with Capturi procesing their data securely and in accordance with applicable regulations.

The Capturi platform was essentially developed after everyone started paying close attention to GDPR due to the introduction of fines. Consequently, Capturi has put the customer and the customers GDPR and security interest at the center of its priorities and the development and operation of the Capturi platform.

This Capturi platform description is intended to be a detailed review of implemented measures that ensures Capturi is perceived and recognized as a vendor that securely processes data on behalf of their customers from all segments, including government and authorities, municipalities, pension funds, banking, utility, and insurance companies.

Should this description give rise to any questions, we are available to answer such by written request to tmb@capturi.com.

# Development method

Capturi is developed based on agile principles with a focus on creating the right solutions in close collaboration with users and customers. Capturi's development department is structured in cross-function teams and works structured with tasks in a dedicated task management system.

All changes to code undergo automated testing as well as review and approval before release. Releases are automatic (CI/CD) several times a day without affecting the running production environment.

The technology stack chosen is the latest languages and modern technologies that ensure high performance, scalability and security.

# Web app

The web app is built as a single page web app in React that communicates securely with Capturi's backend/server over SSL/TLS 1.2 (minimum requirements).

Technologies:

TypeScript / JavaScript / CSS / Web APIs

React / Chakra UI / Emotion / Figma

Turborepo / Lerna / Yarn Workspaces / webpack

ESLint / Prettier

GitHub Actions

# Backend / Server

Capturis backend is built around a number of services that each handle part of Capturi platform. -these services are built so that they easy to scale and act as an *API* for Capturi and other integrations that can be built based on Capturi.

Technologies:

C# / .NET Core / Go / Node.js

MongoDB / RabbitMQ / Redis

Kubernetes / Docker / GitHub Actions

The speech recognizer is a Capturis proprietary model (also referred to as Automated Speech Recognition) developed in Python 3.x and Java 17.x

Note that the Capturi service is a SaaS solution, hence it is operated exclusively on Capturi's environments with full responsibility to ensure updating of versions and frameworks.

# Integrations / API

Using our API, you can connect a wide range of different systems to Capturi, including mail systems, BI systems, customer archives, etc.

As Capturi's core service is analysing conversations, Capturi must have access to its customers' recordings of customer conversations from the systems making those recordings for the customer and e-mails. This is typically the contact center solution such as Puzzel or Genesys, the communications system such as Twillio, Telia or Cisco, or a dedicated recording vendor such as Touch Call Recording or Verint. Capturi *does not* make the recording as part of their service. For e-mails it is the likes of Dynamics, Zendesk, and Dixa the conversations takes place through – e.i. not through Capturi.

Therefore, an integration must be set up that gives Capturi access to the customer's conversations. This integration can for voice basically be done in 2 ways and is often relatively simple.

The easiest way is if there is an API from the recording provider that allows you to directly access the recordings. Alternatively, an FTP or S-FTP server is set up, typically hosted by either the customer, from where the recordings are either sent directly to Capturi by the customer, or from where Capturi can retrieve the recordings.

Capturi integrates to most known systems. Otherwise, the integration work is done as part of start-up, and usually doesn't require great involvement from Capturi's customers. It is a process that is handled solely between Capturi and the customer's supplier making the recordings.

For text it will usually be through an API.

# Data retention

Capturi process the following customer data:

Audio recordings of conversations and e-mails between customers and the customer service agents/employees of Capturi's customers.

E-mail address, photo (users can choose to upload this themselves), number and name of user in Capturi is processed.

Data derived from analyzing the conversations.

Customer data is processed and stored by the following data center providers:

- *Netic A/S ("Netic"), cvr 26762642, Alfred Nobels Vej 25, 9220 Aalborg East, Denmark,* and
- *Hetzner Online GmbH ("Hetzner"), Registration Court Ansbach, HRB 6089, VAT ID No. DE 812871812, Industriestr. 25, 91710 Gunzenhausen, Germany.*

All services associated with the Capturi services, incl. the platform, are mapped. The storage and hosting services provided by Netic and Hetzner do not require the use of other subcontractors, as these services are all performed solely by Netic and Hetzner. All other elements of the Capturi services, incl. the platform, are thus provided directly and exclusively by Capturi with the only exception being Flowmailer BV. They are used to send system e-mails from Capturi (e-mail gateway) and they do not use subcontractors for providing this service. E-mails can, for example, be an invitation to the platform, comments created between users, etc. Flowmailer only processes the user's full name (if this is provided as part of the creation in Capturi) and e-mail addresses.

Capturi has chosen Netic, Hetzner and Flowmailer as suppliers as a consequence of GDPR and *Schrems II*, which make it difficult to use suppliers with connections to third countries, including in particular the US. Obviously, the suppliers are also selected on the basis of their high security measures, certifications and top tier service offerings.

All data, including backup and redundancy environments, is located in either Denmark, Netherlands, Germany or Finland. There are no "follow the sun" support issues. Therefore, Capturi can guarantee our customers that their data is only stored and processed within the EU/EEA.

# System illustration

The illustration included on the next page shows the typical involvement of Capturi customer infrastructure and the interaction with Capturi's infrastructure.

The left side of the illustration shows how audio files flow from the contact center/phone system (similar for e-mails) to Capturi and are processed to make data available to a Capturi user via a browser.

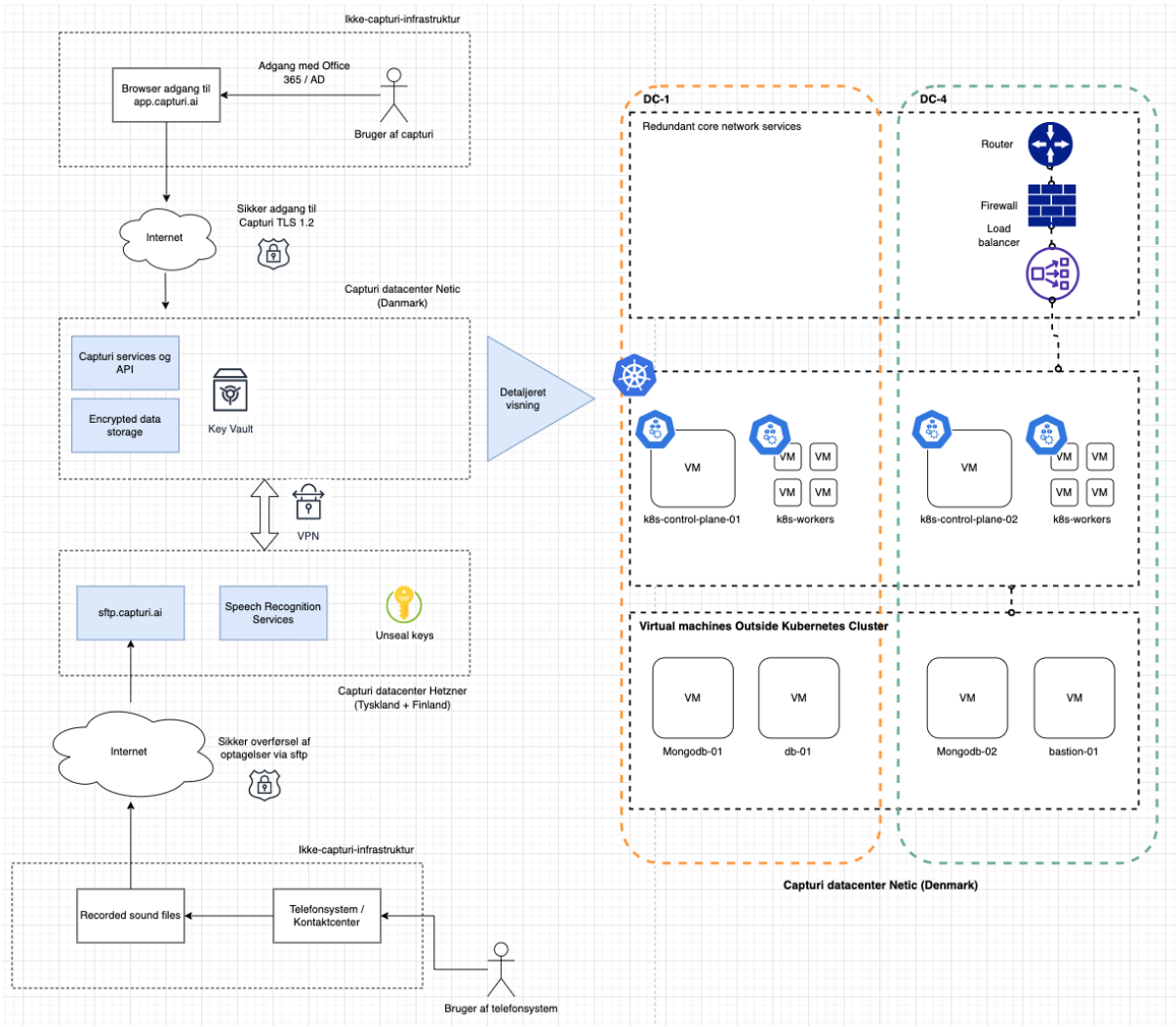
The box referred to as ASR is an expression of Capturi's speech recognition that is operated on a setup with physical machines that are responsible for heavy calculations of data.

The right side of the chart shows a higher level of detail of Capturi's setup by Netic. DC1+4 are the two data centers that together make up the primary infrastructure. Everything is built around a scalable Kubernetes setup that handles the distribution of resources.

The telephone system/contact center and e-mail provider is responsible for recording audio files as well as transferring data to Capturi.

If Capturi host the SFTP server the customer uses to make recordings available to Capturi, this will be at data center Hetzner and all transfers from there are done via secure connection.

The audio files are processed, and data is calculated on Capturi's environment and exhibited via an API, including via the Capturi Web App. The API is accessed in a browser over a secure connection.



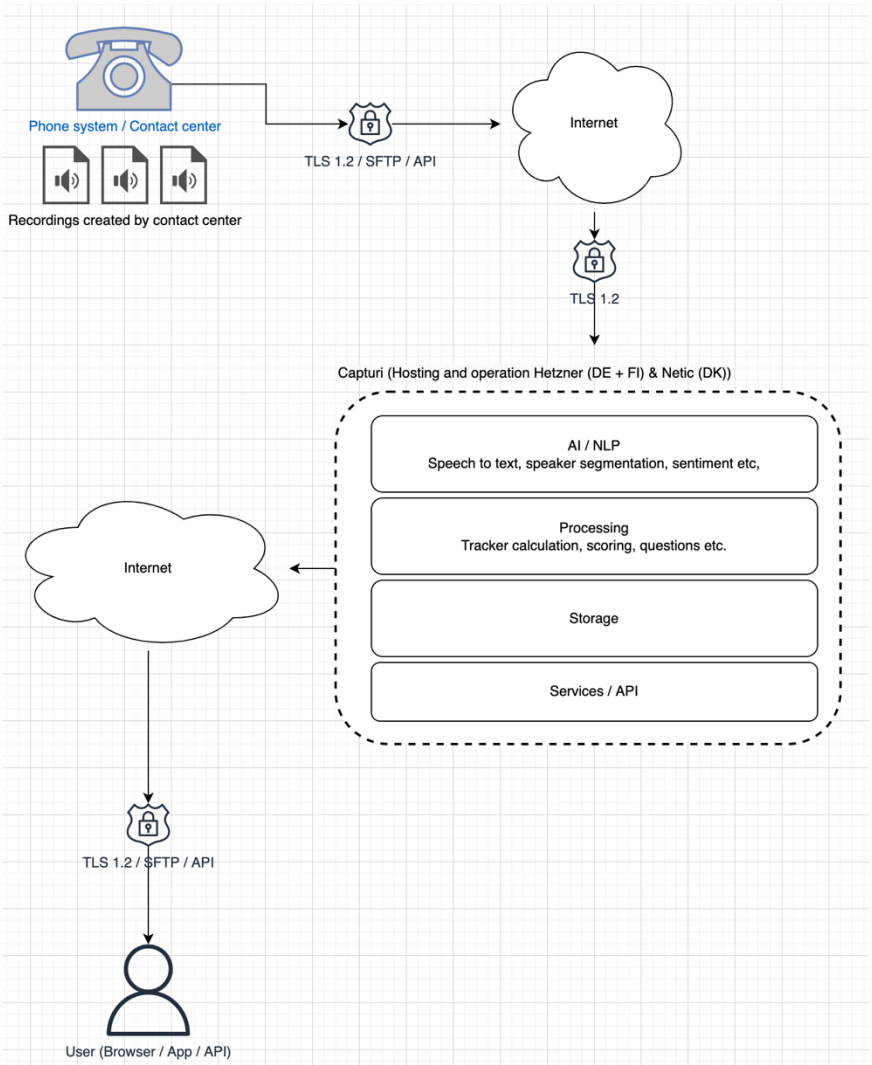

You can see more about Netics and Hetzner's security measures, security certificates, etc. by following these links:

Don't believe: https://www.netic.dk/

Hetzner: https://www.hetzner.com/legal/privacy-policy/

# Processing flow chart

With regard to the processing activities etc. carried out by Capturi as part of Capturi's software service, the following chart provides an overview of the flows, the individual processing operations and by whom and where they are carried out:



**Generative AI based functionality in the Capturi platform, incl. security measures**

We are continuously launching generative AI based functionality to the platform, e.g. our AI summary feature that enables summarization of conversations, which improves the insights and analyses we already make today for the purpose improving and optimize our customers' contact center, customer service, employee training and education, as well as any other customer facing services, including sales services.

All generative AI based functionality in the platform is based on Capturi's use of Microsoft's Azure OpenAI Services. The functionality is optional.

The following security measures have been contractually ensured:

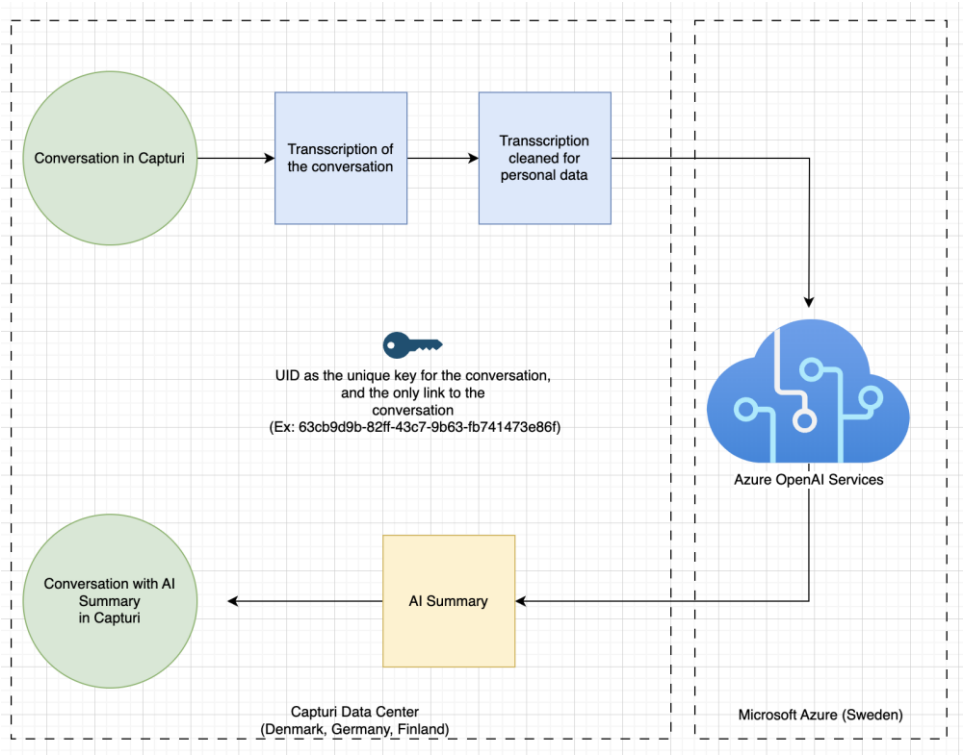
- Microsoft cannot use data or outputs for model training or other purposes,
- Microsoft's processing of data is subject to confidentiality,
- Data is encrypted (in "transit" and "rest"), and
- Data transferred to Microsoft is permanently deleted from their systems after 30 days.

Sweden has been selected as the data location for Microsoft's Azure OpenAI Services.

Any possible transfer of data to the United States will be covered by the EU US Data Privacy Framework - https://www.dataprivacyframework.gov/.

In addition, Microsoft's processing of data, and any potentail transfers to the US, is governed by their Standard Contractual Clauses (November 2023). For details on these, read more here.

Below is an illustration of the dataflow associated with Capturi's use of Microsoft's Azure OpenAI Services:




# GDPR and security measures

## Data retention and recovery

All audio and text files are stored and copied to both our data centers, hence a redundant setup with separate power, network and connection to Capturi.

All data is fully backed up on an hourly, daily, weekly, or monthly basis within each data center region.

Monthly backups are kept 1 month, daily ones are stored for 7 days, weekly ones are stored for 4 weeks and backups for each hour are kept for 2 days.

## Deletion of data

By default, Capturi is set up with a deletion policy so that processed audio and text files, statistics and library audio clips are automatically deleted after certain periods.

Capturi has chosen a default deletion policy setting to ensure that data is deleted in accordance with our customers' obligations under the GDPR. However, it is possible for each customer to change all default settings to reflect their specific deletion requirements and wishes.

Setting up the platform will always involve clarifying the customer's specific requirements, if such have not already been uncovered in the initial discussions between the customer and Capturi, and such agreed deletion policy requirements will be reflected by change of the default settings.

In the following, the various data and related deletion possibilities in the Capturi platform are detailed:

Deletion of data relates to the data that Capturi is processing on behalf of its customers, including:

- recordings of conversations (hereinafter "conversations") between the end-customers and the customer service employees
- e-mail address, photo (user uploads themselves), and name of user in Capturi
- data derived from the analysis of the conversations

Capturi is set up with a default deletion policy that involves:

- Automatic deletion of conversations after 90 days
- Automatic deletion of conversation statistics after 365 days
- Automatic deletion of library audio clips after 1,095 days. It is noted in relation to library audio clips that these have been carefully selected by the customer based on the learning potential of the conversation itself, and adapted so that the clip only includes relevant parts of the conversation, as well as it is possible to select and adapt such library clippings to ensure no sensitive information is included.

Ad. automatic deletion of conversations after 90 days

This implies that the:

- audio and text files of the conversations are deleted so that it is no longer possible to play the conversations

- the word matrix for each conversation contained in the platform's backend (which is the result of transforming the audio recording of the conversation into words, in essence a transcription) is anonymized, whereby the word matrix is irrevocably cleaned of numbers, known names, addresses, and e-mail addresses.

- customer's phone number is deleted

- conversation statistics are kept. By keeping the statistics that in themselves are not relatable to any person, it remains possible to seek out conversations on a given topic. Likewise, it will be possible to see development over time, sentiment, conversation length, conversation reasons, etc.

- Audio snippets in the library functionality is a copy of the relevant snippet from the conversation identified in the platform, hence there will be an audio file of the full conversation in the platform *and* a copy of the audio file that has been chosen to be shared as a good example in the library. From a deletion setting perspective, this means that the audio of the full conversation can be deleted in the platform without the audio snippet in the library is deleted. This is an advantage as the customer does not have to constantly use resources to maintain the library with new sound clips of good examples. It is emphasized that it is possible to select and time-limit the audio clips, so that it is ensured that they contain the least possible personal data.

Please note that the employee's data, including name and audio clips, is kept in the platform, until the customer actively deletes the employee's user profile, e.g. in connection with dismissal of the employee.

Ad. automatic deletion of conversation statistics after 365 days

This default setting means that all words in the word matrix deriving from recordings of conversations older than 365 days is automatically deleted. Thus, it will not be possible to analyze conversations older than 365 days and they will therefore not be reflected in statistics.

Ad. automatic deletion of library audio clips

This default setting means that audio snippets of good examples in the library, that are older than 3 years from the date of introduction into the library, are deleted.

### Possibility of changing Capturi's default deletion setup.

The customer has the possibility of making changes to Capturi's default deletion settings.

The following deletion options can be changed to accommodate deletion policies that deviate from Capturi's default settings:

- period for when conversations should be automatically deleted from the platform
- period for when conversation statistics should be automatically deleted from the platform
- period for automatically deletion of library audio snippets
- whether word matrix should be anonymized in connection with the deletion of audio files of conversations. In the system, it is thus possible to choose between a hard deletion, where both audio file and words in word matrix deriving from the audio file are deleted, or a soft deletion where only audio file is deleted, but words in word matrix is kept clean of all words allowing to link the word or a combination of words to a specific person.

## Can Capturi delete customer data?

In general, data, including user data added by the customer to the Capturi platform, can be irrevocably deleted by the customer's registered users having such deletion rights directly in the platform.

Specific requests for deletion of data, including specific data about users, can also be made with written request to Capturi.

## Does Capturi retain customer data after termination?

Capturi allows customers to export their raw data at any time in industry standards such as JSON for metadata and mp3 for audio format. In addition, customer data may be deleted upon request upon termination as set forth in the section above.

If Capturi does not receive such a request prior to termination, all customer data at Capturi will be automatically deleted within 30 days of the termination of the customer contract.

## Data security and management

Customers' data is stored in our database system, which contains all of Capturi's customer data.

Our database architecture and logical controls are built around a strong guarantee that no customers can access each other's data. Handling of this approach/access is done by using tokens, keys, etc. which

ensures that one customer's data is always kept separate from other customers' data. The way Capturi ensures that this handling is correct is by automated tests that must solved “lighting green" before it is possible to update the solution. Further, all changes and corrections to the platform or database are reviewed and approved before testing begins. Only by accepting changes and completed tests is it possible to run finally run the update.

## Encryption

All data processed by Capturi is encrypted.

During transit of data, *HTTPS* and *TLS 1.2* are used, which ensures that should data be intercepted, it will only be encrypted data the interceptors get access to. For encrypting files that are inactive in our hosting environment, we use strong encryption based on a symmetric master key setup.

Data is processed using strong encryption when data is in rest. The encryption algorithm and its parameterization (e.g., key length or operating mode, etc.) use newest market standard technology, including 256-bit Advanced Encryption Standard (AES-256), which is recognized and recommended by governments and various high security service providers to ensure secure encryption.

Our setup is therefore assessed as being robust against decryption analysis performed by e.g. third parties or states, including by taking into account the resources and technical capabilities (e.g. computing power for brute force attacks) available to them.

Encryption keys are managed safely by Capturi, including in relation to the generation, storage, administration management, and check of identity of an intended recipient with the possibility of revoking.

Unseal keys to our key vault are securely managed by Capturi and stored by Hetzner, our German hosting provider. The keys are therefore not available to anyone other than Capturi.

Capturi has thus implemented a solution where the unseal key for the key vault is stored somewhere other than the data itself and is controlled solely by Capturi.

Customer data is decrypted with the master key in combination with a customer-specific key known only to our encryption and decryption services.

Neither keys nor data in "rest" will at any time be unencrypted. Below is the flow for encryption described in more detail:

## Encryption

- File sent to encryption service
- *Data encryption key* (DEK) for each file is generated using each organization's unique master key
- The file is encrypted with data encryption pin and stored along with master pin id and cipher.

## Decryption

- File loaded from repository
- Master key ID + cipher loaded from the metadata file.
- Cipher is decrypted to a key in vault using the master key ID.
- The file is decrypted using the key

## Access control

Capturi's access to the database and customer data is subject to policies that ensure that customer data can only be accessed if there is a work-related need to do so in relation to Capturi delivering their services to our customers, and that access only applies to selected employees. Management continuously assesses whether employees with access still have a work-related need for such access to customer data.

In addition, employees are trained in what appropriate access includes, and logs of access are kept in accordance with the section below in order to monitor and control any irregular access.

Each employee's access to customer data requires multi-factor authentication (Software MFA - Google Authenticator).

Capturi's password policy assumes that:

- passwords must be at least 8 characters
- they must contain lowercase letters and they must not contain part of the username
- users cannot reuse their passwords.

Capturi's software platform does not have proprietary login functionality, but only allows login with established M365, Google, or Okta user profiles. Capturi therefore has no need to store the user's passwords, and it is thus the chosen login providers' security levels that will also apply to login in the Capturi platform, including, for example, multi-factor authentication.

Full AD integration with Capturi's user administration is on the road map, but is not expected to be released until the first half of 2023.

## Logging

Capturi keeps various logs, including:

- technical monitor for operations
- audit log for change and development of the hosted platform
- audit and user logs for platform actions

## Technical monitor for operation

We log constant response time, CPU load, RAM usage, database read and writes, index usage, and disk usage related to platform activity for the purpose of monitoring availability, response time, failure rate, server load, and more to ensure the platform is always in a healthy state.

Dashboards with this information run in real time and with relevant alerts set up.


## Audit log for hosting platform changes and developments

Capturi employees' access to the backend systems and management console in Netic is logged continuously. An example can be seen below.

The specific log entry is a login from the Admin Console.


```
{
    "kind": "Event",
    "apiVersion": "audit.k8s.io/v1",
    "level": "Metadata",
    "auditID": "8d0dc36f-ea87-4836-984e-71538a127649",
    "stage": "ResponseComplete",
    "requestURI": "/api/v1/namespaces/default/pods?limit=500\u0026resourceVersion=0",
    "verb": "list",
    "user": {
        "username": "https://keycloak.netic.dk/auth/realms/mcs#jhh@netic.dk",
        "groups": [
            "operator_admin",
            "operator_user",
            "system:authenticated"
        ]
    },
    "sourceIPs": [
        "77.243.49.62"
    ],
    "userAgent": "k9s/v0.0.0 (linux/amd64) kubernetes/$Format",
    "objectRef": {
        "resource": "pods",
        "namespace": "default",
        "apiVersion": "v1"
    },
    "responseStatus": {
        "metadata": {},
        "code": 200
    },
    "requestReceivedTimestamp": "2022-01-20T10:14:24.117312Z",
    "stageTimestamp": "2022-01-20T10:14:24.117823Z",
    "annotations": {
        "authorization.k8s.io/decision": "allow",
        "authorization.k8s.io/reason": "RBAC: allowed by ClusterRoleBinding \"oidc-operator-admin\"
        of ClusterRole \"cluster-admin\" to Group \"operator_admin\""
    }
}
```


In addition, all releases and/or code changes are logged and stored so that all changes can be traced back in time in the event that there is a need to recreate previous versions of the platform.

## Audit and user logs for platform actions

Logging actions in the platform is based on user interactions and is divided between an *audit log* and a *usage log*, each serving their own purpose.

The audit log is the log containing events performed by the user that Capturi wishes to store within the framework of Capturi's deletion policies as agreed with the customer. The purpose is to be able to track who has performed what actions in the platform. The log includes conditions such as successful login, changing user permissions, playing conversations, deleting conversations, deleting trackers, etc.

It is noted that since Capturi uses external login providers, Capturi does not have a real login session, but relies on authentication from the login provider. Capturi therefore alone logs all successful sessions.

Logging of expired tokens, modified tokens, and deactivated tokens is constantly monitored.

Below is an example of a successful login on the platform:


```
{
    "_id" : ObjectId("5fda059e0f66a90fe28aceb2"),
    "dateTime" : ISODate("2020-12-16T13:03:26.923Z"),
    "ip" : "77.66.28.33",
    "loginProvider" : "google",
    "loginSucceeded" : true,
    "userName" : [redacted],
    "error" : "",
    "requestId" : "1608123806744:authentication-6cd6c66bbb-z2m4q:1:kirep6z9:10676"
}
```


Usage logging is functional usage monitoring. The purpose of this logging is to further product development in the interest of the customer based on a deeper understanding of the customers' actual use of the platform and Capturi's performance.

# User roles and privileges in Capturi

In Capturi, there are four types of roles. The role defines what data you can see and access in the platform as well as what rights you have in relation to configuration of the platform.

Each role comes with a number of default configuration privileges . These rights can, if necessary, be adjusted for the individual user (see section 'rights')

## Description of the four user roles

### Owner

- The 'Owner' role can both access and see all data in the platform. This means that an 'owner' can access conversations and see data on all employees in the organization.

- The 'Owner' role has the right to set up and configure all parts of the platform, including 'trackers', 'segments', etc. (see more under the section 'Rights').

- In addition, the 'Owner' role is the only role to have access to the user management page. Thus, only the 'Owner' role can create, edit, invite and deactivate users, including editing the individual user's rights in the platform.

- Also, only the 'Owner' role can configure teams and change agents' team affiliation.

### Administrator

- The 'Administrator' role can access and view all data in the platform. This means that an 'Administrator' can access conversations and see data on all employees in the organization.

- By default, the 'Administrator' role has the right to set up and configure all parts of the platform, including 'trackers', 'segments', etc. (see more under the section 'Rights').

- The 'Administrator' role differs from the 'Owner' role by *not* having access to the user management page.

### Team Leader

- The 'Team Leader' role can access and view conversations and data within the team for which he or she is a team leader (team and leader role determined by the platform Owner), and thus cannot access conversations outside the team or see data for these, including names of other employees.

- By default, the 'Team Leader' role has the right to set up and configure all parts of the platform, including 'trackers', 'segments', etc. (see more under the section 'Rights').

### User

- The 'User' role only has access to and view data on their own conversations

## User privileges

Each role comes with a set of default privileges. These rights can, if necessary, be adjusted for the individual user.

Below is the default setup for each role, as well as which privileges it is possible to change at user level by the platform “Owner”:

*Default privileges for the 'Owner' role:*

- can access the 'user management' page. However, an 'Owner' cannot edit their own user in relation to rights – this can only be done by Capturi.
- can play conversations across the platform (privilege can be removed)
- can create, edit and delete:
    - dashboards (privilege can be removed)
    - trackers (right can be removed)
    - segments (right can be removed)

    - scores (right can be removed)
    - library playlists (right can be removed)

- can download audio files for the individual conversation (right can be removed)
- can download audio file for the individual library audio clip (right can be removed)
- can create comments

*Default privileges for 'Administrator' role:*

- can play conversations across the platform (privilege can be removed)
- can create, edit and delete:
    - dashboards (privilege can be removed)
    - trackers (right can be removed)
    - segments (right can be removed)
    - scores (right can be removed)
    - library playlists (right can be removed)
- can download audio files for the individual conversation (right can be removed
- can download audio file for the individual library audio clip (right can be removed)
- can create comments

*Default privilegies for 'Teamleder' role:*

- can play conversations within your own team (right can be removed)
- can create, edit and delete:
    - dashboards (privilege can be removed)
    - trackers (right can be removed)
    - segments (right can be removed)
    - scores (right can be removed)
    - library playlists (right can be removed)
- can create comments

*Default privileges for the 'User' role:*

- can play your own conversations (privilege can be removed)
- can create, edit and delete:
    - segments (right can be removed)
    - library playlists (right can be removed)
- can create comments

*Link to video walk through of user rights section in the platform (5 mins):*

https://www.loom.com/share/7d7511871e5449219c69bc397cae8964

# HR/company policies

Capturi runs background checks on all employees or contractors who will work for Capturi before starting up work for Capturi. In addition, it is ensured that such individuals have sufficient qualifications to be able to safely perform the tasks in question. Further, all employees and relevant contractors having access to customer information as part of performed services, signs confidentiality agreements that ensure that any customer information is kept confidential.

Capturi uses subcontractors to provide the software service to Capturi's customers. In addition to the obligations related to switching or adding new subcontractors in the dedicated data processing

agreements, Capturi has a fixed policy for choosing new suppliers, which ensures that only suppliers with high security standards are selected.

## The Danish state's minimum technical requirements (2023)

Capturi continuously considers the minimum technical requirements imposed on Danish government authorities and ensures that the requirements for each minimum requirement are complied with when designing Capturi's safety measures – this is ensured by following the compliance criteria set out in the guideline instructions published by the Danish state.

# GDPR

The customer is the data controller for the personal data added by the customers to the Capturi platform and data created in the platform. Capturi is the data processor of the customers data for the purpose of providing the Capturi software services to the customers. Capturi is thus subject to the instructions of the customer for such processing.

The requirements for Capturi's processing of personal data on behalf of customers, and the parties' relations in relation thereto, are regulated in a separate data processing agreement, and Capturi never begins processing until such a data processing agreement has been agreed with the customer.

Capturi’s data processing agreement is based on the Danish Data Protection Agency's standard data processing agreement, which ensures that the requirements for a valid data processing agreement, cf. GDPR, Article 28, are met.

Capturi's customers have full control over what information they add to the Capturi platform and are obliged to ensure the legality and legal basis for using Capturi for the purposes requested by the customer.

Capturi values GDPR compliance and is dedicated to enabling our customers to comply with their obligations as data controllers under the GDPR.

## Audits and security certifications

Capturi stores customer data with our hosting providers, cf. the section above, all of which have annual audits based on the following internationally recognized standards e.g. ISAE 3402, ISAE 3000 or SOC reports.

Capturi also makes an ISAE 3000 auditor's report - based on the use of Capturi’s standard data processing agreement - available to Capturi's customers for the purpose of their control of us as a data processor and our compliance with GDPR and the data processing agreement.

## Threat and vulnerability management

Patching and updating of the production environment is carried out by our trusted hosting providers in close cooperation with Capturi.

The hosting environment is protected by anti-malware scanning software.

Capturi periodically engages ethical hackers for manual penetration tests.