celonis

Whitepaper
Task Mining & Privacy by Design

As of April 2024

Introduction

Customer use cases for Celonis Task Mining depend on privacy and employment laws, as well as company policies, applicable to each customer. Therefore, the core of Celonis' Task Mining Technology is designed according to the requirements of **Privacy by Design,** supporting our customers to execute and manage the software in line with their privacy policies.

This white paper gives an overview of the **multiple safeguards** which are available to provide **maximum control** at the customer's end. The document also provides input for activities that might be helpful to mitigate potential concerns raised by stakeholders.

Additional information on data privacy and information security as well as **certifications** (e.g. ISO 27001, ISO 27701) can be found on the Celonis website: www.celonis.com/trust-center/.

What are the specifics of Celonis Task Mining?

With the **Celonis Platform**, Celonis offers a state-of-the-art process mining tool for analyzing event data of source systems (e.g. ERP solutions).

With Celonis **Task Mining**, user interaction with multiple applications used to complete a task or process can be analyzed. The Task Mining software runs on a user's desktop, and is activated when a specific application is used. The collected data (e.g. clicks, scrolls) is then uploaded to Celonis Platform for detailed analysis. By analysing **User Interaction Data** on how users allocate their time among different applications, it is possible to gain insights into employee experiences and inefficiencies.

Celonis Task Mining software is designed to focus on understanding how specific work is performed by examining the **patterns at large** in order to optimize, improve and automate the task/process, not to focus on the individual(s) completing them.
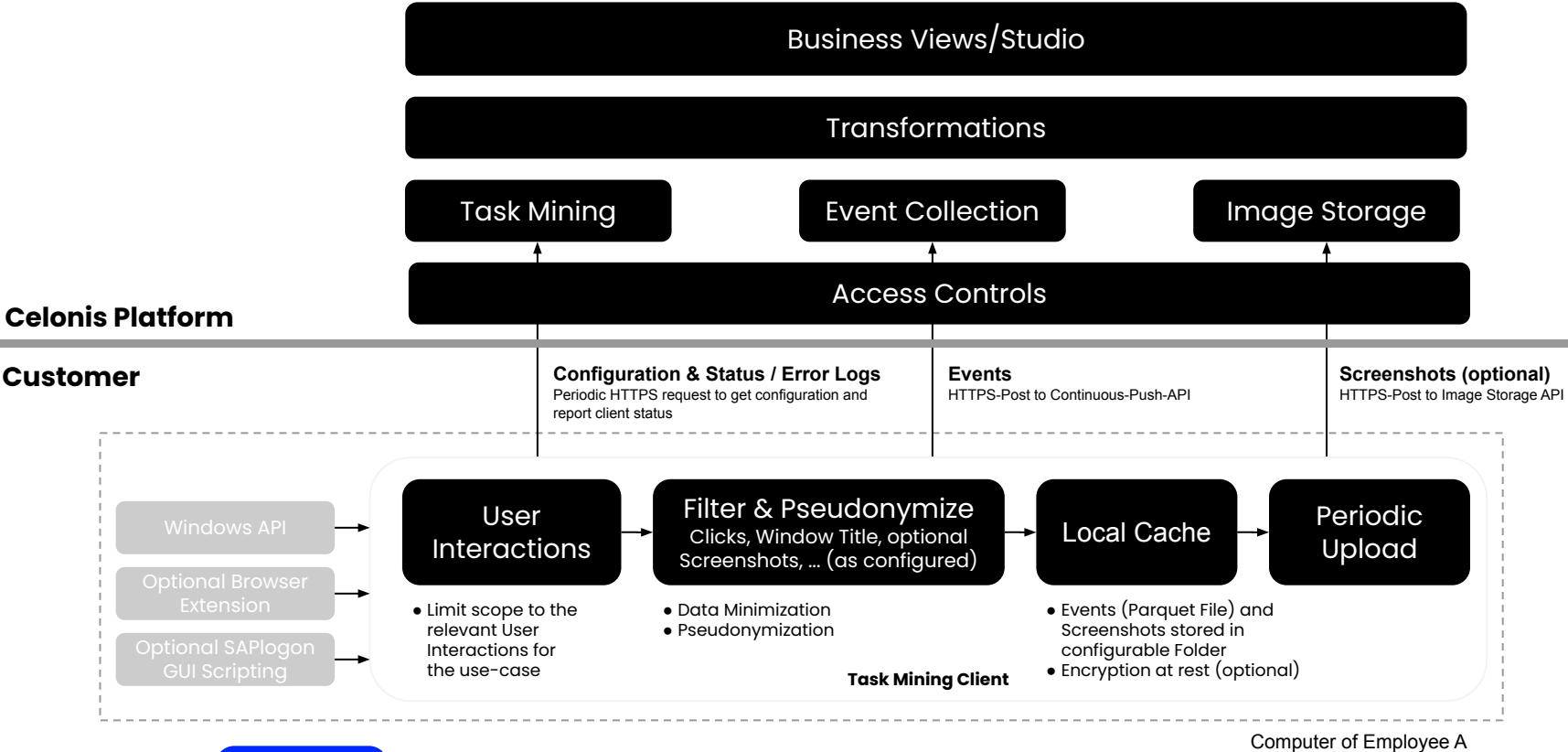
Architectural Overview

Business Views/Studio

Transformations

Task Mining

Event Collection

Image Storage

Access Controls

Celonis Platform

Customer

Configuration & Status / Error Logs
Periodic HTTPS request to get configuration and report client status

Events
HTTPS-Post to Continuous-Push-API

Screenshots (optional)
HTTPS-Post to Image Storage API

Windows API

Optional Browser Extension

Optional SAPlogon GUI Scripting

User Interactions

Filter & Pseudonymize
Clicks, Window Title, optional Screenshots, ... (as configured)

Local Cache

Periodic Upload

● Limit scope to the relevant User Interactions for the use-case

● Data Minimization
● Pseudonymization

Task Mining Client

● Events (Parquet File) and Screenshots stored in configurable Folder
● Encryption at rest (optional)

Computer of Employee A

Introduction

Task Mining Basics

Privacy Controls

Summary

What is Privacy by Design?

C

Data Privacy or Data Protection by Design is an approach to systems engineering which demands that privacy principles are taken into account throughout the whole engineering process.

Data protection through technology design was specifically included into multiple legal frameworks such as the EU General Data Protection Regulation (**GDPR**) and the California Consumer Privacy Act (**CCPA**). Software providers (Processors), shall develop products and services that allow their customers (Controllers) to configure them in a manner that ensures compliance with applicable legal requirements.

Celonis Task Mining has been designed and developed in close cooperation with our **data privacy experts** to ensure that the privacy requirements are considered throughout the product lifecycle. Further developments and new features are assessed in privacy checks that are an integral part of our product development process.

Overview: Enterprise-Ready Privacy Controls for Celonis Task Mining

System Tray Notification
Users have transparency of the data collected and can pause Task Mining at any time.

Information Screen
Users are informed about details and purpose of the Workforce Productivity project.

Application filters
Allowlist and denylist applications limit data collection to the application on scope of the analysis.
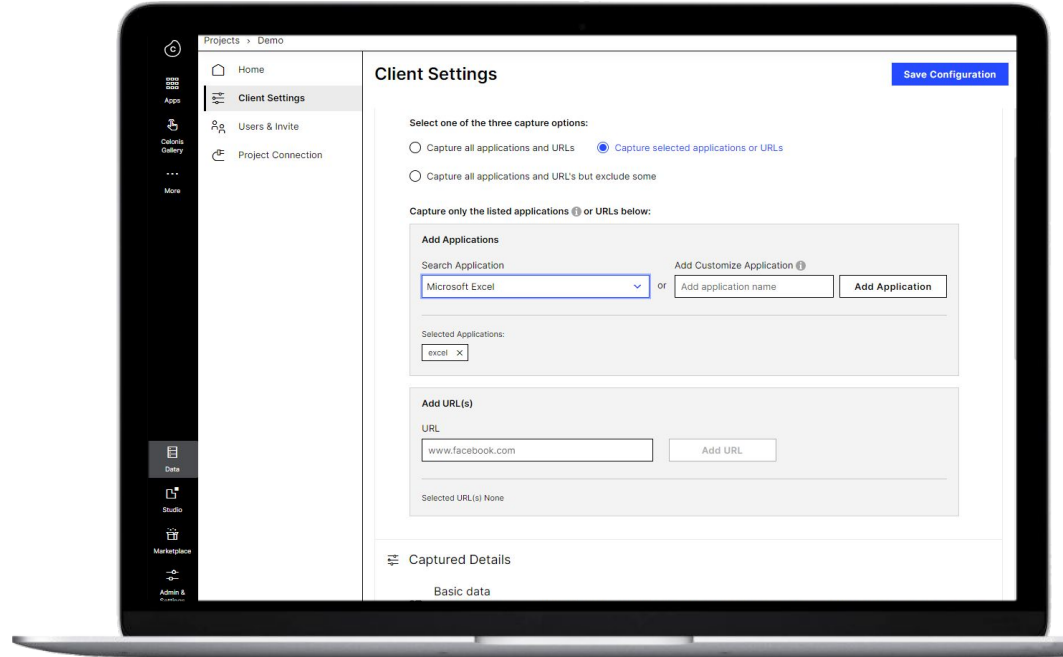
Attribute capturing & reduction
Select attributes per application reduce the data to the minimum required by the specific use case.

Pseudonymization
Controls are in place to pseudonymise usernames and other personal information to protect individuals.

Granular Access Rights
Only selected individuals can access the analysis to avoid misuse of information.

Projects > Demo

Home
Client Settings
Users & Invite
Project Connection

Apps

Celonis Gallery

More

Client Settings

Save Configuration

Select one of the three capture options:

○ Capture all applications and URLs   ● Capture selected applications or URLs
○ Capture all applications and URL's but exclude some

Capture only the listed applications ⓘ or URLs below:

Add Applications

Search Application   Add Customize Application ⓘ
[Microsoft Excel   ▾]   or   [Add application name]   [Add Application]

Selected Applications:
[excel ×]

Add URL(s)

URL
[www.facebook.com]   [Add URL]

Selected URL(s) None

⚏ Captured Details

Basic data

Data

Studio

Marketplace

Admin &

Lawfulness, Fairness and Transparency – System Tray

For transparency, the fact that Task Mining is running is displayed in the system tray of the user.

By clicking on the tray, users can check the settings and see the details on the interactions captured via their desktop.

The user can also pause Task Mining via the system tray at any point in time.
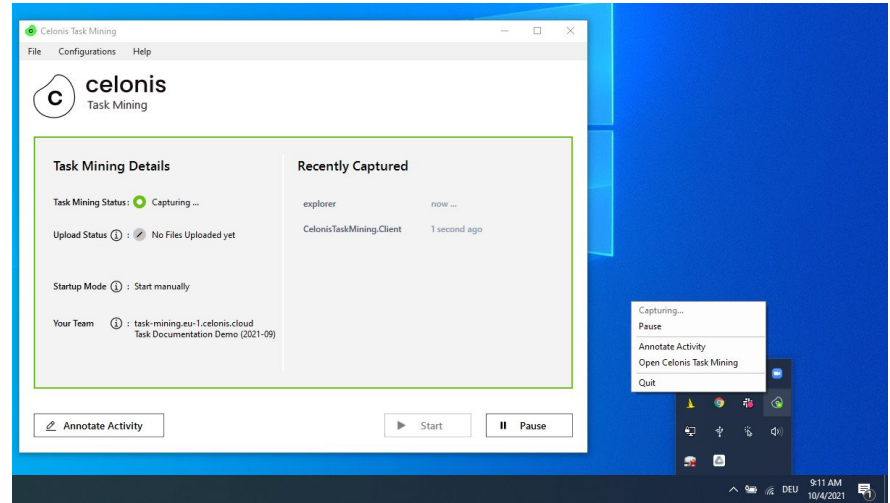
Lawfulness, Fairness and Transparency - Information Screen

In order to provide the information/notice required by certain employment and privacy laws, an information screen pops up directly after the installation of the software on the user's device and before the initial collection of any data.

Per organisation, the content of the screen can be configured based on the specific use case and provide information on the planned processing of the data to be collected.

Data Minimization & Purpose limitation
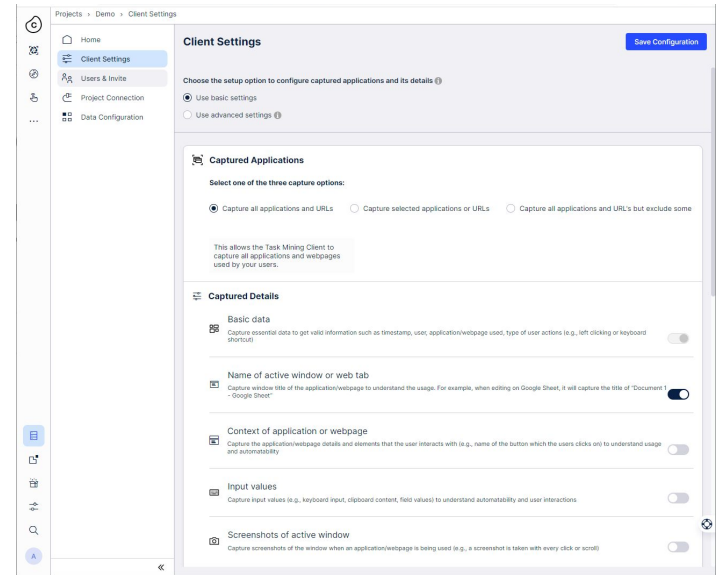# - Application Filters

Celonis Task Mining is designed to limit data collection and processing to the relevant data categories required for the analysis. Events which do not satisfy the rules will not be collected.

There are several levels for limiting the data collected:
- Select or exclude single applications
- Collect minimal context such as the window title, general headline, etc. or solely that a certain application was used without further details
- Deactivate text input and screenshots

Celonis Task Mining provides full configuration flexibility per use case as the settings can be configured for each purpose individually.
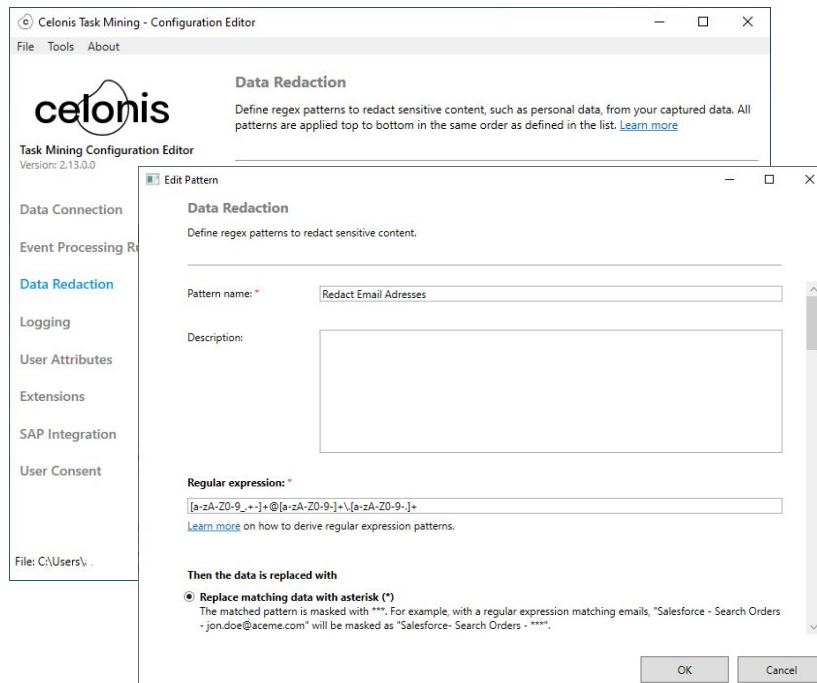
Data Minimization & Purpose limitation - Attribute Capturing and Redaction

Celonis Task Mining can be configured by the admin to capture only specific data points or not to capture specific data points at all (such as Window Titles, URLs, Computer Name, etc.).

Also a one way (non-reversible) hash using the family of Secure Hash Algorithms (SHA) can be applied to certain data points captured, e.g. window title. The SHA hash is irreversible. There is no lookup table to reverse this process.

Alternatively, specific patterns can be anonymized by replacing the data with '***', e.g. to always redact Credit Card Numbers and/or email addresses.

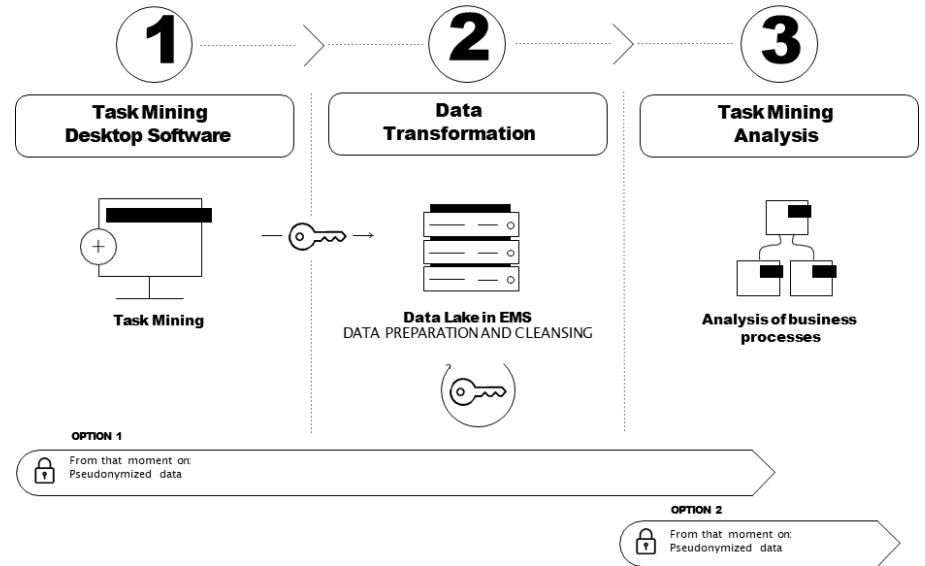| Introduction | Task Mining Basics | **Privacy Controls** | Summary |

Data Minimization & Purpose Limitation - Pseudonymization

Celonis Task Mining provides granular controls to specify which of the data categories collected should be pseudonymized, e.g., usernames, entered text, clipboard content, application path and/or application title, name of active windows or elements. In this case, personal data will be converted into non-trackable hash-values by algorithms from the SHA family.

Data can be pseudonymized on the desktop software (directly while capturing user interactions in the Task Mining Desktop Software) and/or during data transformation (when uploading it to the database within the Celonis Platform).

1

Task Mining Desktop Software

Task Mining

2

Data Transformation

Data Lake in EMS
DATA PREPARATION AND CLEANSING

3

Task Mining Analysis

Analysis of business processes

OPTION 1
From that moment on:
Pseudonymized data

OPTION 2
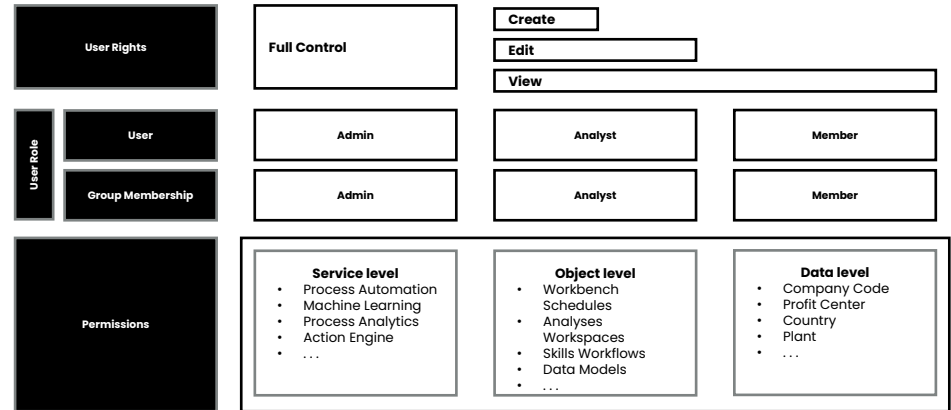From that moment on:
Pseudonymized data

Confidentiality
– Granular Access Rights

C

A detailed, role-based authorization concept means that data and information access can be limited to authorized users.

User access to objects and elements can be specified with user and group permissions. Access to single data points in an analysis can be restricted using a comprehensive data permissions framework.

User Rights		Full Control		Create
				Edit
				View

User Role	User	Admin	Analyst	Member
	Group Membership	Admin	Analyst	Member

Permissions	Service level	Object level	Data level

	• Process Automation
	• Machine Learning
	• Process Analytics
	• Action Engine
	• . . .
		• Workbench
		  Schedules
		• Analyses
		  Workspaces
		• Skills Workflows
		• Data Models
		• . . .
			• Company Code
			• Profit Center
			• Country
			• Plant
			• . . .

Communication is key!

C

A successful Task Mining implementation highly depends on stakeholders' early engagement and acceptance.

Therefore it's crucial to properly mitigate concerns of stakeholders, not only by technical safeguards but also by complementary organisational measures, such as comprehensive communication efforts.

Task Mining focuses on understanding how specific work is performed in order to optimize, improve and automate the process.

The focus is on the work and patterns at large, not the individual executor.

Ahead of the processing

Which data will be collected and how will it be used and shared?

During the processing

Which potential process improvements have already been achieved identified?

After the processing

How did the processing of the user's data serve the purpose(s)?

Legal Disclaimer

This document is provided for **informational purposes only**. It represents Celonis' current product offerings and practices as of the date of issue of this document, which are subject to change without notice. Customers are solely responsible for independently assessing the information contained in this document.

This document does not create any warranties, representations, contractual commitments, conditions or assurances from Celonis, its affiliates, suppliers or licensors, and it does not provide legal advice. Celonis' sole obligations are as described in the applicable contract(s) between it and its customers, and this document is not part of, nor does it modify, such contract(s).

celonis

Thank you!

privacy@celonis.com