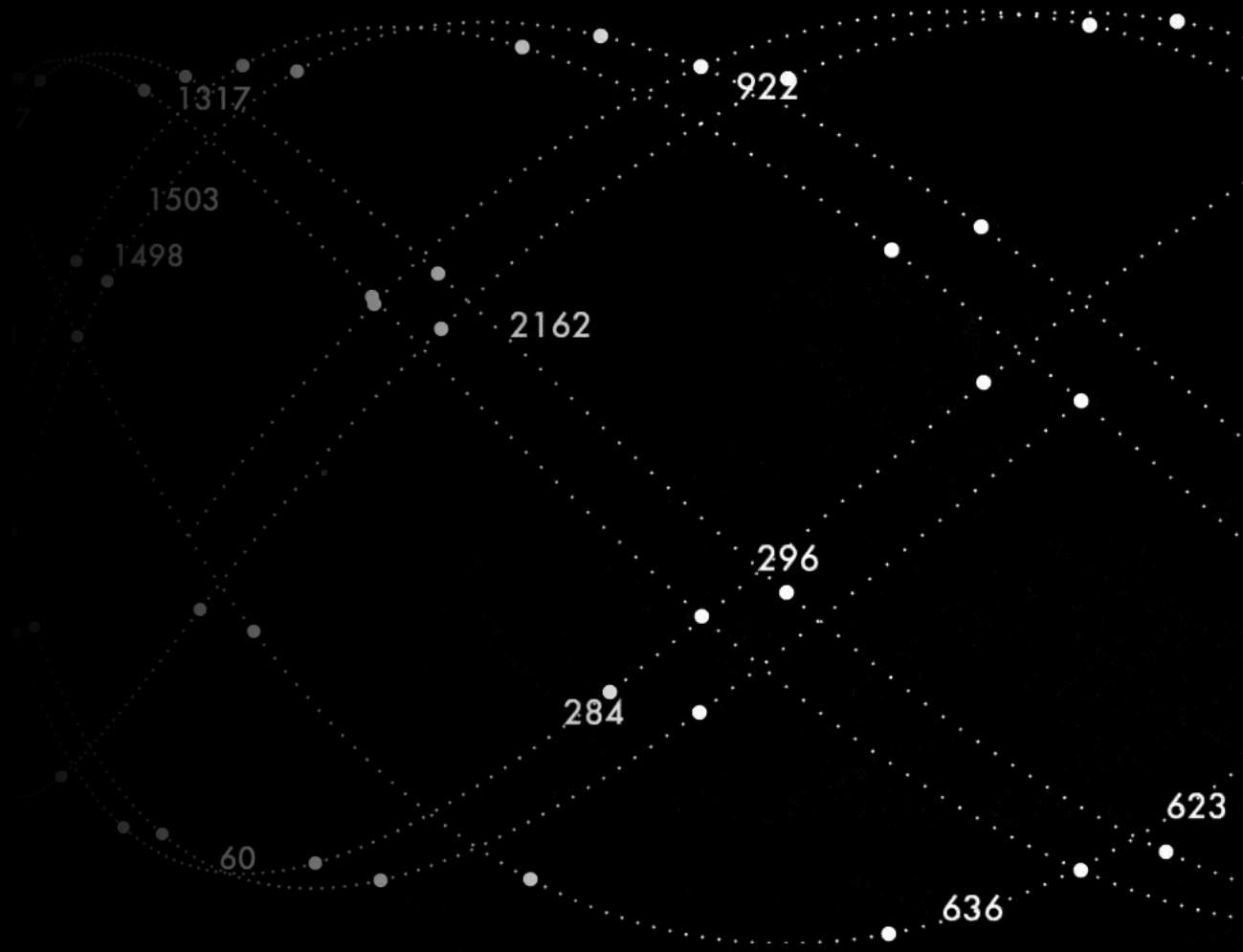
Data Privacy by Design

Celonis EMS



Introduction

- Powered by its market-leading process mining core, the Celonis Execution Management System provides a set of applications, and developer studio and platform capabilities for business executives and users to eliminate billions in corporate inefficiencies.
- Celonis helps you as the controller of the personal data analyzed within the EMS to execute GDPR-related data privacy policies your organization might set up through its Privacy by Design approach. (cf. Chapter 11)
- Additionally, Celonis has taken multiple efforts to ensure compliance with GDPR within its organization, providing you with the assurance that Celonis is a trustworthy processor of all your personal data (cf. Chapter 111).
- The fact that numerous customers - including several public authorities and publicily-owned companies (e.g. ABB, AstraZeneca, Coca- Cola, Citibank, Danaher Corporation, Dell, GSK, John Deere, L'Oréal, Siemens, Uber, Vodafone) - already are successfully using Celonis Process Mining technology confirms the high standards of Celonis' software Customers (cf. Chapter IV).

Data Protection by Design

01

Lawfulness, Fairness and Transparency

The EMS helps you to process personal data lawfully, fairly and in a transparent manner in relation to the data subject.

02

Purpose Limitation

The EMS supports the need to collect personal data only for a specific, explicit and legitimate purpose and only as long as necessary to complete this purpose.

03

Data Minimization

- In order to visualize as-is processes in Celonis, there is no inherent need to process user information or personal data.
- The depth of the analyses can be adjusted flexibly within the data provision and setup of the analyses by yourself (limiting the data procession by privacy by default with configuration at set up possibilities) helping you to minimize the use of personal data within EMS.

Data Protection by Design

04

Accuracy & Accountability

Through repeated synchronization with your Source System, we assist your efforts to keep all personal accurate and up to date in your systems. The set up of the EMS as shown in the other principles supports your effort to be fully accountable for the use of personal data within the EMS.

05

Storage Limitation

Once personal data are no longer required to operate analyses within the EMS (including in the event of termination of your subscription) you can request the deletion of all personal data within the EMS, which also operates with a predefined deletion concept. Additionally, you are able to delete all data referring to your account at any time with a request to Celonis, to ensure compliance with the purpose limitation.

06

Integrity and Confidentiality

Following the data thrift, no personal data will be used that is not explicitly needed for the analyses. In case user information is needed (e.g. for reviewing the dual control principle), this data will be pseudonymized. It is also possible to anonymize data. Industry best practice security mechanisms ensure data processed is safeguarded.

01 Lawfulness, Fairness and Transparency

- The GDPR requires **you as the controller of the personal data processed** within the EMS to process such personal data "lawfully, fairly and in a transparent manner in relation to the data subject".
- All processing activities within the EMS are properly logged, allowing you to **clearly identify to which extent personal data have been processed.** Where required (which should be an exception as all personal data on the EMS are originating from your own source system), Celonis can support access requests of data subjects in accordance with applicable law on basis of and in compliance with a data processing agreement.
- This ensures full **transparency** and compliance with the GDPR.

02 Purpose Limitation and 03 Data Minimization

- Data collected for different purposes can be processed for the intended use only and in compliance with the predefined purpose. First and foremost, a selection of relevant/uncritical data depending on process and analysis focus is possible. **Pseudonymization or anonymization of sensitive data is also supported.**
- Celonis processes personal data within the platform only to a limited extent. In order to visualize the as-is processes in Celonis, there is **no need for user information or personal data.**

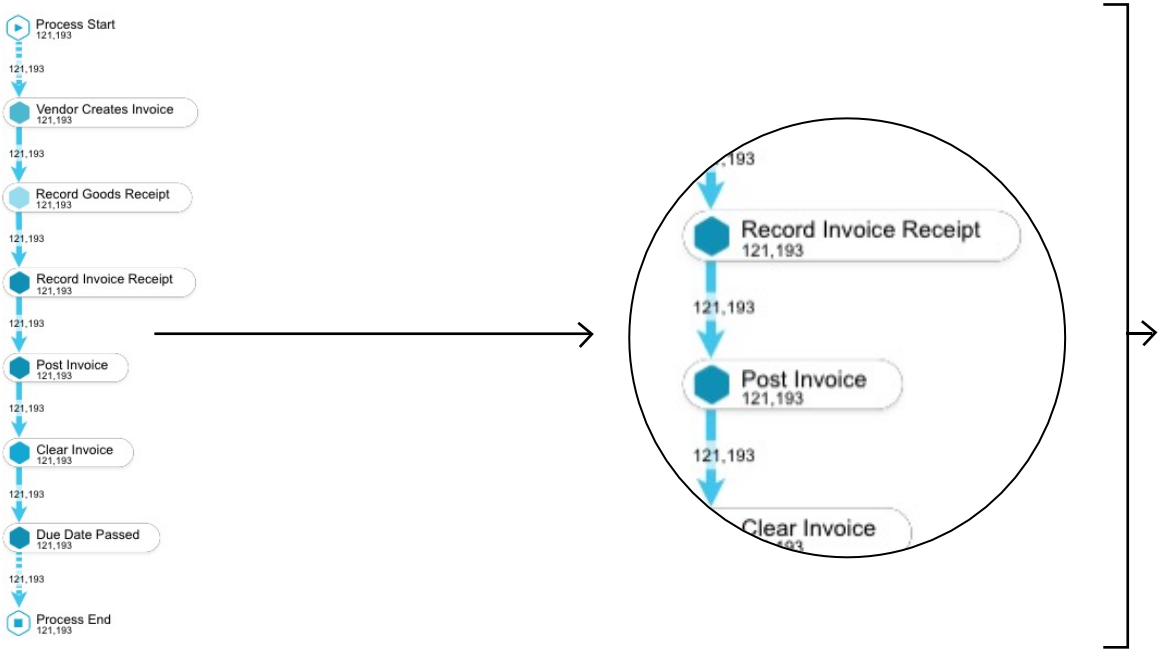
02 Purpose Limitation and 03 Data Minimization

- User information and user authentication in the Celonis Execution Management System are limited to username and email address to identify the user. Both **can be set, changed and deleted** by the user himself and are not exposed to others.
- The **depth of the analyses can be adjusted** flexibly with the data provision and setup of the analyses by the controller in the configuration. There is no need to include critical user information from the source system. The authorization concept is whitelisting users for data objects and analyses. Access to data, view on data assets and analysis can be **restricted with highest granularity and in compliance with the need to know principle** and in accordance with the intended use and purpose limitation. **A differentiated authorization concept** at company level ensures **user-specific restriction of analysis.**

02 Purpose Limitation

Celonis Process Mining

Process Analysis/Details



What is Process Mining? What are the necessary prequisites?

- Pure Process Analysis
- Usage of existing data, no need for re-collection of data
- No need for personal data

02 Purpose Limitation & Authorization Concept

Login via SSO / SAML and 2 Factor Authentication

Authorizations in Celonis →

Role based Access-Management

Viewer

- Responsibilities: evaluation and process analysis within his field of activity and responsibility
- A viewer has only **reading rights** and is only able to analyze areas under his responsibility

Analyst

- Responsibilities: Creation of analyses/ reports, definition of key figures
- An analyst has the same authorization as a viewer plus the authorization to build analyses and reports (**writing rights**)
- An analyst's authorization is restricted to the user's area of activity

Data Scientist

- Responsibilities: Connection of new processes and data sources
- A data scientist's authorization is the same as for an analyst with additional **writing rights on the data model**

A **differentiated authorization concept** at company level allows to ensure **user-specific restriction of analysis authorization** at various levels (e.g. accounting area, region, etc.).

03 Data Minimization

Pseudonymization

Sample data:
User: Max Mustermann
User. Erika Mustermann
User: Max Mustermann
User: Max Mustermann

Sample data:
User: 44aa488f0
User: 8f261ba7
User: 44aa488f0
User: 44aa488f0

Same values are mapped to the same values.

Data Security/Personalised Data

- Option I: Pseudonymization is happening **directly during data extraction**. To achieve this goal Celonis pseudonymizes the data on the fly, hence ensuring that the plaintext data never leaves the underlying system
- Option 2: **All personalized data** will be **pseudonymized** in the **database**, making it available in the analyses only pseudonomized
- All personalized data will be **converted** into **non-trackable hash-values** (green)
- Pseudonymization is done by using a **Hash algorithm of the SHA-3.**

04 Accuracy and Accountability

- The GDPR principles require you as the controller of personal data to keep any personal data **accurate and up to date.**
- As data for analysis in Celonis is necessarily pulled, **access to accurate process data** is granted by the customer by the customer who is controller of the processed personal data.
- Through ongoing Synchronization of the EMS with your Source System, all personal data is being **kept in sync with your source system,** i.e. if there is a correction in the Source System, it will be directly applied on the Celonis platform, **helping you to achieve compliance with this accuracy requirement of the GDPR.**

04 Accuracy and Accountability

- Celonis Process Mining provides a range of possibilities to ensure that you
- **meet accountability requirements,** i.e.
  - as shown before, the minimization of personal data in use by purpose related configuring of the analyses set up, offering transparency through properly logging all processing activities within the EMS
  - allowing you to clearly identify to which extent personal data have been processed and
  - guarantee subject requests for data deletion and accessibility granting the accuracy of processed data by synchronization with the source system in both directions

...due to our **Privacy by Design** setup of the solution and privacy by default through offering a high granularity in configuration possibilities.

04 Accuracy and Accountability

01 → **02** → **03** → **04** → **05** → **06**

Lawfulness, Fairness and Transparency

Purpose Limitation

Data Minimization

Accuracy

Storage Limitation

Integrity and Confidentiality Authentication

- The features and functionalities of EMS as shown in the previous principles displayed, **supports your effort to be fully accountable for the use of personal data you process** within the EMS.

05 Storage Limitation

- GDPR principles oblige you to keep all personal data in a form which permits identification of data subjects for **no longer than is necessary** for the purposes for which the personal data are processed and in compliance with the initial purposes.
- You are **able to delete** any source data from the EMS at any point in time by yourself or by request to Celonis.
- We support this requirement further through automatic deletion of all remaining customer data related to all installed customer accounts (including personal data) once your Subscription Term has ended. All data is only kept as long as necessary for the purpose of performing the agreement. Additionally, you will be able to extract your data instance prior to such deletion as mentioned in your contract in order to **adhere to any storage and/or other retention requirements.**
- Celonis has implemented robust deletion concepts and timeliness which ensure a consistent approach to data deletion.

06 Integrity and Confidentiality

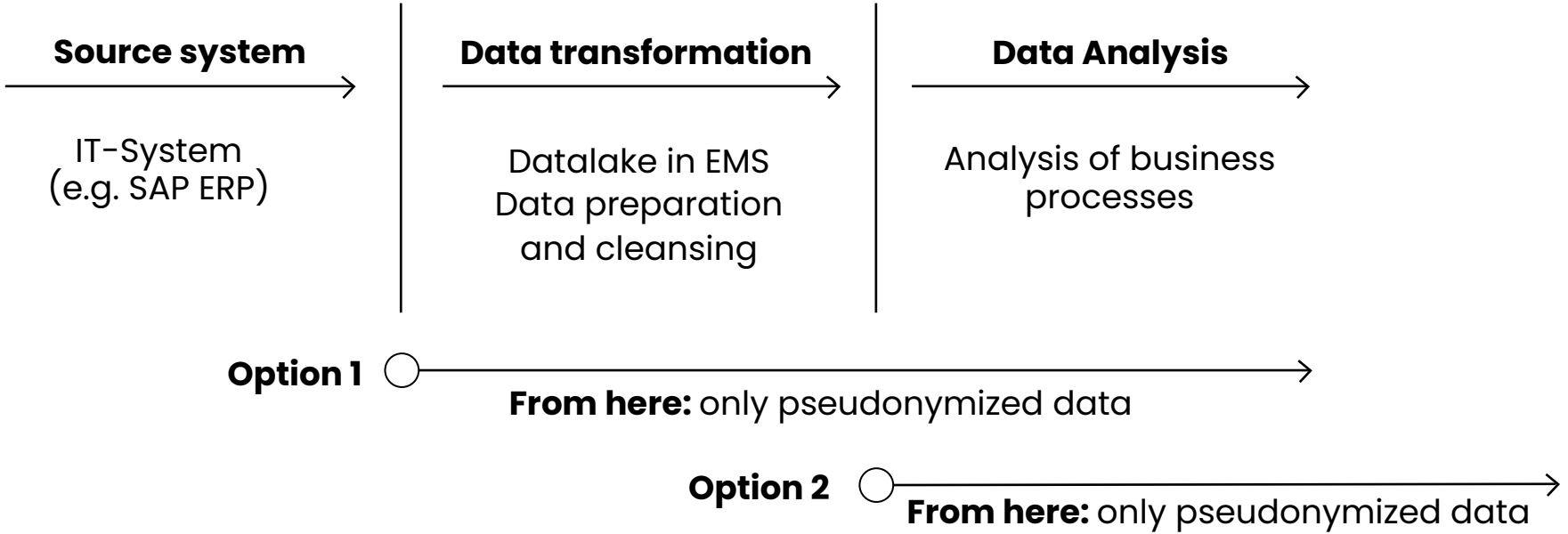
- Celonis acknowledges that you are required to **process all personal data** in a manner that **ensures appropriate security confidentiality and authentication** of the personal data **using appropriate technical or organizational measures.**
- Celonis has a 2-factor authentication mechanism that can be activated by a customer. Additionally, an **IP range logging** in the access form can be added so that only people from the local network can log on. The **authorization concept** is **whitelisting users for data** objects and analyses (see details on user management) .

06 Integrity and Confidentiality

- **Where personal data are needed** to be processed in the EMS for process analyses purposes upon your request, for example to ensure compliance to the dual control principle, this **data can be used in an anonymized or pseudonymized format.**
- For this approach **two options** exist:
  a) Pseudonymization or **anonymization in the data replication pipeline**
  b) Pseudonymization or anonymization **directly on the analytics database.**

  For details, see the next page.

06 Integrity and Confidentiality



Data can be pseudonymized during data extraction (Option 1) or during data transformation (Option 2).

Data Protection Compliance as a Company

Data Protection Policies

Celonis has created and actively uses data processing procedures, website policies, a data protection policy and a detailed data protection manual.

Supplier Audit

Celonis continuously monitors its suppliers to ensure supplier agreement are in compliance with GDPR, including in view of any processing activities which may be carried out outside the EEA.

Data Protection Officer

A data protection officer for Celonis and its European subsidiaries has been appointed.

Self-Assessment

The overall efforts taken by Celonis as an organization, including a required self-assessment conducted together with our data protection officer, ensure compliance with the GDPR.

Training

All Celonis employees are trained on a recurring basis regarding data protection compliance.

ISO Certification

Celonis has obtained a certification of its information security systems in accordance with ISO 27001, and is ISO 9001:2015 certified.

Addendum

Selected European Customers

Publicly-owned companies/Public Sector/Trade Unions

Industrial Sector

- Successful examination and active usage in more than 250 companies (amongst others 30% of all DAX companies)
- Declaration of consent by various workers' councils, inter alia Deutsche Telekom and Bayerischer Rundfunk

Selected European Customers

This document is provided for informational purposes only. It represents Celonis's current product offerings and practices as of the date of issue of this document, which are subject to change without notice. Customers are responsible for making their own independent assessment of the information in this document and any use of Celonis's products or services, each of which is provided "as is" without warranty of any kind, whether express or implied.

This document does not create any warranties, representations, contractual commitments, conditions or assurances from Celonis, its affiliates, suppliers or licensors. The responsibilities and liabilities of Celonis to its customers are controlled by Celonis agreements, and this document is not part of, nor does it modify, any agreement between Celonis and its customers.

Thank you.

Contact details
www.celonis.com