CELONIS
PROCESS MINING

IBC - DATA PRIVACY BY DESIGN

I. INTRODUCTION

With its Process Mining Technology Celonis offers a state-of-the-art tool for **analyzing business processes** within the company. By **visualizing the as-is processes**, Celonis supports companies in simplifying existing processes and thereby increasing their **efficiency and quality**. Having optimized processes leads to **increased employee satisfaction**, too.

When using the Process Mining Technology, Celonis helps you as the controller of the personal data analyzed within the Intelligent Business Cloud to execute **GDPR**-related data privacy policies your organisation might setup through its Privacy by Design approach (cf. Chapter II).

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 III).

The fact that numerous customers - including several public authorities and publicily-owned companies (e.g. Bayerischer Rundfunk, Deutsche Telekom, Deutsche Bahn, IG Metall) - already are **successfully using Celonis‘ Process Mining technology** confirms the **high standards** of Celonis‘ software Customers (cf. Chapter IV).

How the Celonis IBC helps You to comply with the GDPR key principles through Privacy by Design

1	**Lawfulness, Fairness and Transparency**	The IBC helps You to process personal data lawfully, fairly and in a transparent manner in relation to the data subject.
2	**Purpose Limitation**	The IBC 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.
3	**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, helping You to minimize the use of personal data within the IBC.

II. CELONIS INTELLIGENT BUSINESS CLOUD – DATA PROTECTION BY DESIGN

4 Accuracy	Through repeated synchronization with Your Source System, we assist Your efforts to keep all personal data You control accurate and up to date, also within the IBC.
5 Storage Limitation	Once personal data are no longer required to operate analyses within the IBC (including in the event of termination of Your subscription) You can request the deletion of all personal data within the IBC, which also operates with a predefined deletion concept.
6 Integrity and Confidentiality	Following the concept of 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.
7 Accountability	The set up of the IBC as shown in the other principles supports Your effort to be fully accountable for the use of personal data within the IBC.

1 LAWFULNESS, FAIRNESS & TRANSPARENCY

The GDPR requires **You as the controller of the personal data processed** within the IBC to process such personal data “lawfully, fairly and in a transparent manner in relation to the data subject“.

All processing activities within the IBC 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 IBC are originating from Your own source system), Celonis can support access requests of data subjects in accordance with applicable law.

This ensures full **transparency** and compliance with the GDPR.

2 PURPOSE LIMITATION AND 3 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.**

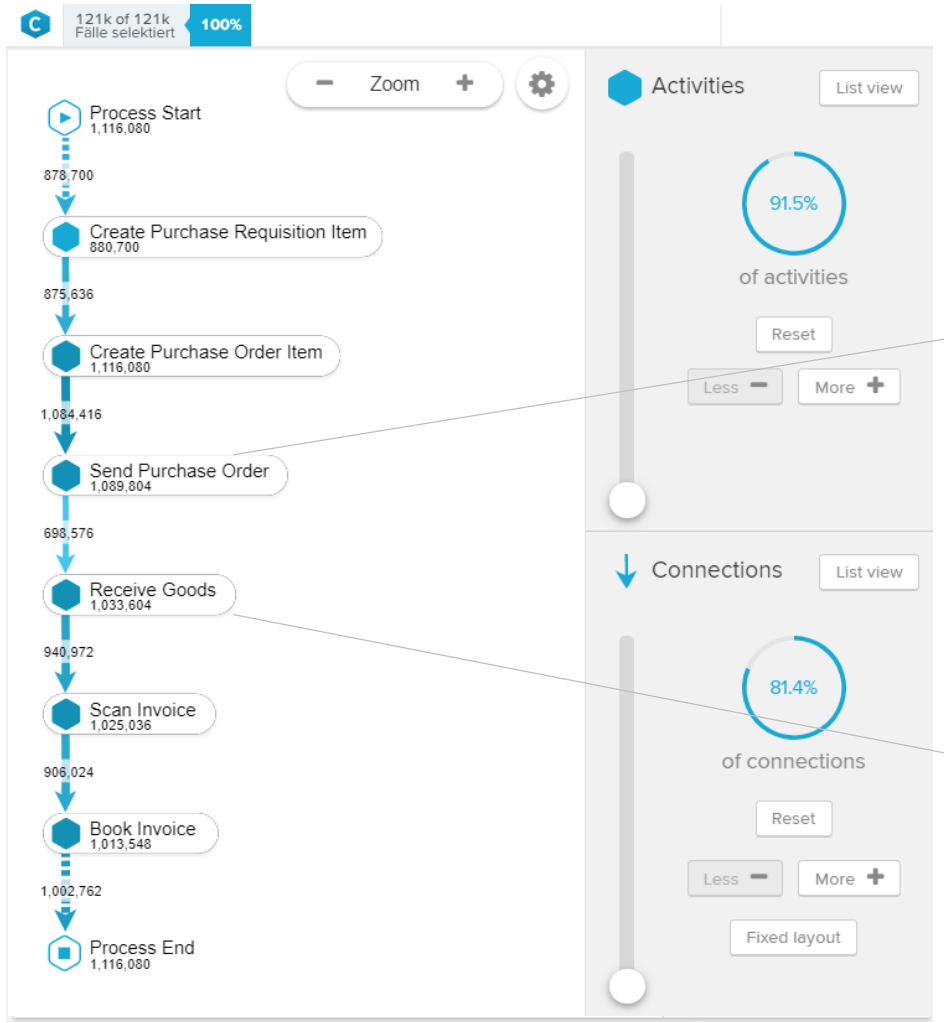
Celonis processes personal data within the platform only to a very limited extent. In order to visualize the as-is processes in Celonis, there is **no need for user information or personal data**. User information and user authentication in the Celonis Intelligent Business Cloud are limited to username and mail 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. 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. A **differentiated authorization concept** at company level ensures **user-specific restriction of analysis**.

For details, see the next three slides.

2 PURPOSE LIMITATION

CELONIS PROCESS MINING



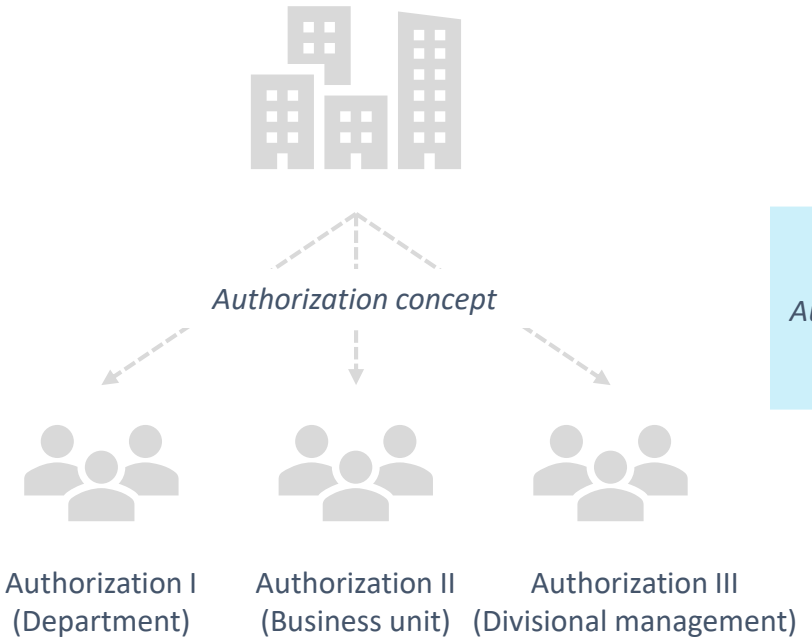
PROCESS ANALYSIS / DETAILS

What is Process Mining? What are the necessary prerequisites?

- ✓ Pure process analysis
- ✓ Usage of existing data, no need for re-collection of data
- ✓ No need for personal data

2 PURPOSE LIMITATION & AUTHORIZATION CONCEPT

USER MANAGEMENT VIA LDAP[1)]



Authorizations in Celonis

USER MANAGEMENT @ CELONIS

Viewer

- ✓ Responsibilities: evaluation and process analysis within his field of activity and responsibility
- ✓ A viewer has only **reading rights** and is able to only 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.).

[1)] Lightweight Directory Access Protocol

3 DATA MINIMIZATION

PSEUDONYMIZATION

Pseudonymzation

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

Pseudonymization of data

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

Equal values are mapped to equal values.

DATA SECURITY / PERSONALISED DATA

- ✓ Option 1: Pseudonymization is happening **directly during data extraction.** To achieve this goal a SAP function module is used, that pseudonymizes the data on the fly, hence ensuring that the plaintext data never leaves the SAP 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 SHA1/2** family

4 ACCURACY

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.

Through ongoing Synchronization of the IBC 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 requirement**.

5 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.

You are **able to delete** any source data from the IBC at any point in time.

We support this requirement further through deletion of all remaining customer data (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. Of course, You will be able to extract Your data instance prior to such deletion 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.

6 INTEGRITY AND CONFIDENTIALITY

Celonis acknowledges that You are required to **process all personal data** in a manner that ensures **appropriate security of the personal data using appropriate technical or organisational measures**.

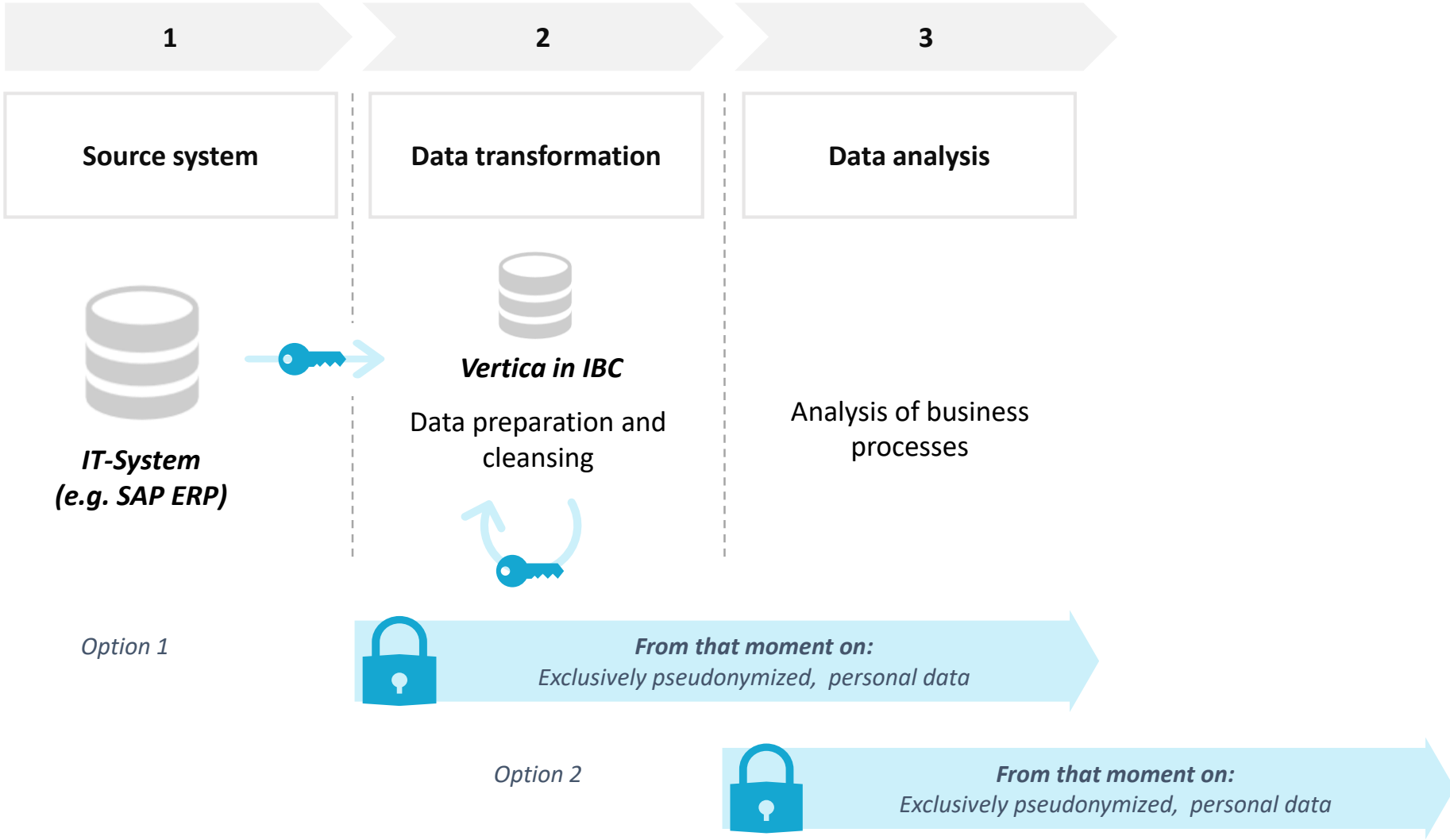
Celonis has a 2-factor authentication mechanism that can be activated by a customer. Additionally, an **IP range logging** in the access form can be added so that only people from the local network can log on. The **authorization concept is whitelisting** users for data objects and analyses (details on user management also see page 11) .

Where personal data are needed to be processed in the IBC 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 slide.

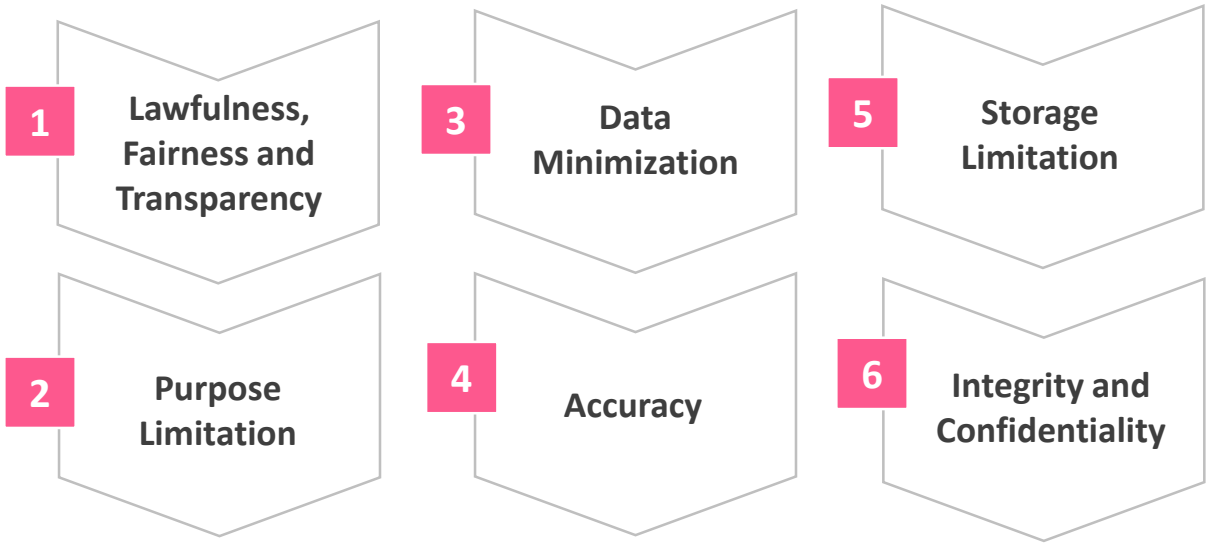
6 INTEGRITY AND CONFIDENTIALITY



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

7 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, that all processing activities within the IBC are properly logged, allowing you to clearly identify to which extent personal data have been processed and guarantee subject requests for data deletion and accessibility due to our **Privacy by Design** setup of the solution.



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

Celonis has undertaken significant efforts to ensure its compliance with GDPR and information security requirements as an organization, including but not limited to:

Data Protection Policies

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

Data Protection Officer

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

Training

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

Supplier audit

Celonis has completed a supplier audit to ensure supplier agreement are in compliance with GDPR, including in view of any processing activities which may be carried out outside the EEA.

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.

ISO Certification

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

celonis

PUBLICLY-OWNED COMPANIES / PUBLIC SECTOR / TRADE UNIONS

DB · IG Metall · BR · SWR · NDR · WDR · Öffentliche Versicherung Braunschweig

INDUSTRIAL SECTOR

SIEMENS · LANXESS Energizing Chemistry · vodafone · Bayer · ABB · EDEKA · MR · MAPAL

T · RWE · klöckner & co · KNAUF · WACKER NEUSON · AIRBUS · SCHOTT

- ✓ **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

DISCLAIMER

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.