PREDEFINED USE-CASE FRAMEWORK: BUSINESS PARTNER DATA MANAGEMENT ("BPDM")

7 MARCH 2024

VERSION 1.0

KEY PRINCIPLES FOR BPDM ("USE CASE")

This document sets out the predefined use case framework (**"Framework"**) for each participant in this Use Case (**"Participant"**). Participants must agree to this Framework and make their data exchange legally binding by way of separate declarations. This document does not specify or restrict how Participants make such declarations.

Each Data Provider / Data Consumer (as a legal entity acting with proper authorization) must register for this Use Case in order to conclude data exchange contracts with the help of a registered connector.

Unless otherwise set out below, defined terms are those set out in the 10 Golden Rules.

1. KEY PARAMETERS

1.1 WHO WITH WHOM?

[Data Provider may tie certain access authorizations (**"Access Policies"**) to its data offers for one or several Data Consumers. By limiting access to certain Participants, Data Provider maintains control over its anti-trust obligations when sharing certain data. In particular, Data Provider may apply Access Policies to restrict access to a particular data offer for only one Participant identified by a specific business partner number (**"BPN"**).]

Participants are companies active in the CX Data Space (including, without limitation, companies providing core services (**"Operating Companies"**)). For the sake of clarification and the purposes of this Use Case, Operating Companies may also function as Data Providers and/or Data Consumers.

1.2 HOW, WHAT AND WHY?

[Data categories by (i) technical description and (ii) data quality parameters (if any)]
[Additional characteristics of data quality]
[Scope of usage right(s)]

Participants provide and use the data in compliance with the standards set by the Association (https://catena-x.net/en/standard-library):

Unless otherwise agreed individually, Participants expressly exclude any requirements for quality, coherence, completeness of data; Data Provider provides data in its respective state "as is" and "as available".

Data Consumer may use the data in line with the agreed purpose(s) and not for other purposes.

*For each data set, Participants may agree on the standardized purposes below (**"Predefined Purposes"**).*

*Data Provider may grant access and/or transfer the data to affiliates ((affiliated companies within the meaning of Section 15 German Stock Corporation Act, AktG, **"Affiliates"**), if Affiliates as Data Consumers submit to the rules under this Framework as applicable between Data Provider and Data Consumer.*

Predefined Policy (*for registering data assets in the connector*)	**Typically used for Data Model**	**Further information on data exchange between Data Provider and Data Consumer**	**Predefined Purpose**
Data Verification, Curation and Enrichment cx.bpdm.gate.upload:1	Gate Data Model	"Upload" Operating Company as Data Consumer uses data to create a record of basic information about entities active in the automotive industry and assigning a BPN to each of those.	Verifying, curating, and enriching data to create a record of basic information about all entities with a BPN in the CX Data Space accessible to all Participants ("**Golden Record**") and for early warning services (value-added services, "**VASs**").
cx.bpdm.gate.download:1	Gate Data Model	"Download" Operating Company as Data Provider provides data from the Golden Record ("**Business Partner Data**") as an alternative source of information for Data	Providing basic information about entities with a BPN in the CX Data Space for Data Consumer to identify counterparty and/or for VASs.

		Consumer about its potential counterparty.	
Business Partner Golden Record cx.bpdm.pool:1	Pool Data Model	"Download" Operating Company as Data Provider provides Business Partner Data from the Golden Record to Participant as Data Consumer to identify other Participants within the CX Data Space.	Identifying Participants within the CX Data Space for Data Consumer's internal counterparty identification and information processes and/or for VASs.
Data Quality Dashboard ("**DQD**") cx.bpdm.vas.dataquality.upload:1	BP data model	"Upload" Operating Company as Data Consumer screens Data Provider's Business Partner Data to assess data quality.	Screening Data Provider's data (i) to assess Data Provider's data quality and (ii) to create benchmarks for future screenings of other Participants' data by Data Consumer to fulfill the goals of the DQD application.
DQD cx.bpdm.vas.dataquality.download:1	DQD data model	"Download" Operating Company as Data Provider provides screening result for Participant as Data Consumer.	Data Consumer assessing quality of own data.
Bank Data Verification Dashboard (**BDV**) cx.bpdm.vas.bdv.upload:1	Gate & BDV Data Model	"Upload" Operating Company as Data Consumer screens Data Provider's bank data.	Screening relevant Data Provider's bank data to verify Data Provider's bank data.
Bank Data Verification Dashboard (**BDV**)	BDV Data Model	"Download" Operating Company as Data Provider provides	Verifying Data Consumer's submitted bank data.

cx.bpdm.vas.bdv.download:1		BDV screening result data to Participant as Data Consumer	
Fraud Prevention Screening Dashboard (**FPD**) cx.bpdm.vas.fpd.upload:1	FP Data Model	"Upload" Operating Company as Data Consumer screens Business Partner Data for fraud prevention screening purposes.	Screening Data Provider's business partner data to assess fraud.
Fraud Prevention Screening Dashboard (**FPD**) cx.bpdm.vas.fpd.download:1	FP Data Model	"Download" Operating Company as Data Provider provides FPD screening result to Participant as Data Consumer	Data Consumer assessing fraud risks when transacting with another Participant.
Sanction Watchlist Screening Dashboard (**SWD**) cx.bpdm.vas.swd.upload:1	Gate Data Model	"Upload" Operating Company as Data Consumer screens Business Partner Data for sanction watchlist screening purposes.	Screening Data Provider's beneficial ownership data to assess trade compliance.
Sanction Watchlist Screening Dashboard (**SWD**) cx.bpdm.vas.swd.download:1	SWD Data Model	"Download" Operating Company as Data Provider provides SWL screening result to Participant as Data Consumer	Data Consumer assessing trade sanction risks when transacting with another Participant.
Natural Person Screening Dashboard ("**NPS**") cx.bpdm.vas.nps.upload:1	Gate Data Model	"Upload"	Verifying Data Provider's Business Partner Data against natural person data entries.

		Operating Company as Data Consumer Operating Company screens Business Partner Data for erroneous natural person data (e. g.: checks if data submitted for entity should be "*Max Miller GmbH*" instead of "*Max Miller*")	
Natural Person Screening Dashboard (**NPS**) cx.bpdm.vas.nps.download:1	NPS Data Model	"Download" Operating Company as Data Provider Operating Company as Data Provider provides NPS screening result data Data Consumer downloads screening result.	Data Consumer verifying its own Business Partner Data.
Country Risk cx.bpdm.vas.countryrisk:1	Country Risk Data Model, Gate and Pool Data Models	Business Application Provider as Data Provider uses Business Partner Data to provide country risk application	Screening Participants' business data to identify risks when collaborating with a new/existing business partner according to official or company-specific country risk assessments.

1.3 WHEREFROM AND WHERETO?/CONFIDENTIALITY

[Locations of data source and data processing (EU / non-EU)]

[Confidentiality]

Participants are free to agree individually. However, geographical limitations may apply, as specified and updated from time to time by the Association ("white list").

Participants are free to agree confidentiality requirements individually. However, a restriction applies that Data Consumer may provide access to data internally (and including for permitted Affiliates) on a need-to-know basis only.

1.4 COMPLIANCE

[Data Provider and Data Consumer must clarify relevant checkpoints in advance, e.g. antitrust law, export control, trade secrets, data protection, etc.].

Data Provider and Data Consumer are responsible for compliance with all legal and regulatory requirements applicable (in particular with regard to (i) antitrust law (including, but not limited to, antitrust-compliant implementation taking into account the "one-up-one-down principle" and "compliance by design"), (ii) tax, trade and export control law, (iii) data protection, (iv) trade secrets, digital regulation) for themselves and any Affiliates registered for this Use Case.

1.5 EXIT

[Return / Deletion of data].

Default setting "keep" or "delete" according to this Use Case.

Existing data exchange contracts remain unaffected, if a Participant withdraws its registration from this Use Case or terminates its contract with an operating company.

1.6 HOW LONG?

[Duration of (i) contract, (ii) data provision and (iii) usage right(s)]

The (i) data exchange contract term, (ii) Data Provider's obligation to provide data and (iii) Data Consumer's usage right(s) each end on 16 October 2024, unless ending later as agreed individually.

Unless agreed otherwise individually, Data Consumer must delete data within 14 days after its usage right(s) has/have ended.

Unrestricted Freedom of Contract

outside of elements 1.1 - 1.6 above

1.7 CONSEQUENCES OF MALPERFORMANCE

[Participant's rights, liability and limitations; depending on the nature of the data exchange contract under applicable law, statutory law may govern Participant's rights, liability and limitations; (Core/Onboarding) service providers may provide default positions for this Use Case, while Participants are free to deviate from such default positions].

Unless otherwise agreed, Data Consumer's rights in case of malperformance are excluded to the extent legally possible.

1.8 MISCELLANEOUS

[preconfigured depending on the contractual relationship under civil law; (Core/Onboarding) service providers may provide default positions for this Use Case, while Participants are free to deviate from such default positions].

Data Provider and Data Consumer are free to agree individually on any other element (e.g. choice of law/place of jurisdiction) in their data exchange contract.