SAGE

Regulatory Compliance Through SAGE

Mark Dietrich, Technical Coordinator, SAGE

Bloodstone Consulting OÜ

SAGE

The Data Space for a Sustainable Green Europe

Co-funded by the European Union

Co-funded through the Digital Europe Programme (DIGITAL)
Grant agreement № 101195471

Key Aspects of Reg Compliance

Monitoring

- Reporting entities responsible for their own data collection
- But many entities need data from their own suppliers
- SAGE supports data re-use across the supply chain with data sovereignty (using Data Sharing Groups)
- SAGE supports small and large participants through upcoming versions of Eclipse Dataspace Connector

Reporting

- Reporting == structured, trusted data exchange between reporting entity and public authority
- Structured → semantic compliance, enforced by SAGE data onboarding rules
- Trusted → SAGE validates identities of both reporting entity and public authority, log of data exchange available to both parties
- SAGE supports public authority with upward reporting (e.g. MS to EU), open data (per DGA), value-added services for reporting entities

Verification

- Contents of reports audited by certification bodies, who issue digital credentials as proof of their certification (W3C: VC/VP)

Co-funded through the Digital Europe Programme (DIGITAL)
Grant agreement № 101195471

SAGE

Near Term Regulatory Applications of SAGE

- UC1: Forestry (EUDR B2G declarations + B2B certifications)*
- UC5: Circular Textiles (ESPR/DPP traceability)*
- UC4: CO_2 Hub (CSRD disclosures)*
- UC9: Natural Capital reporting*

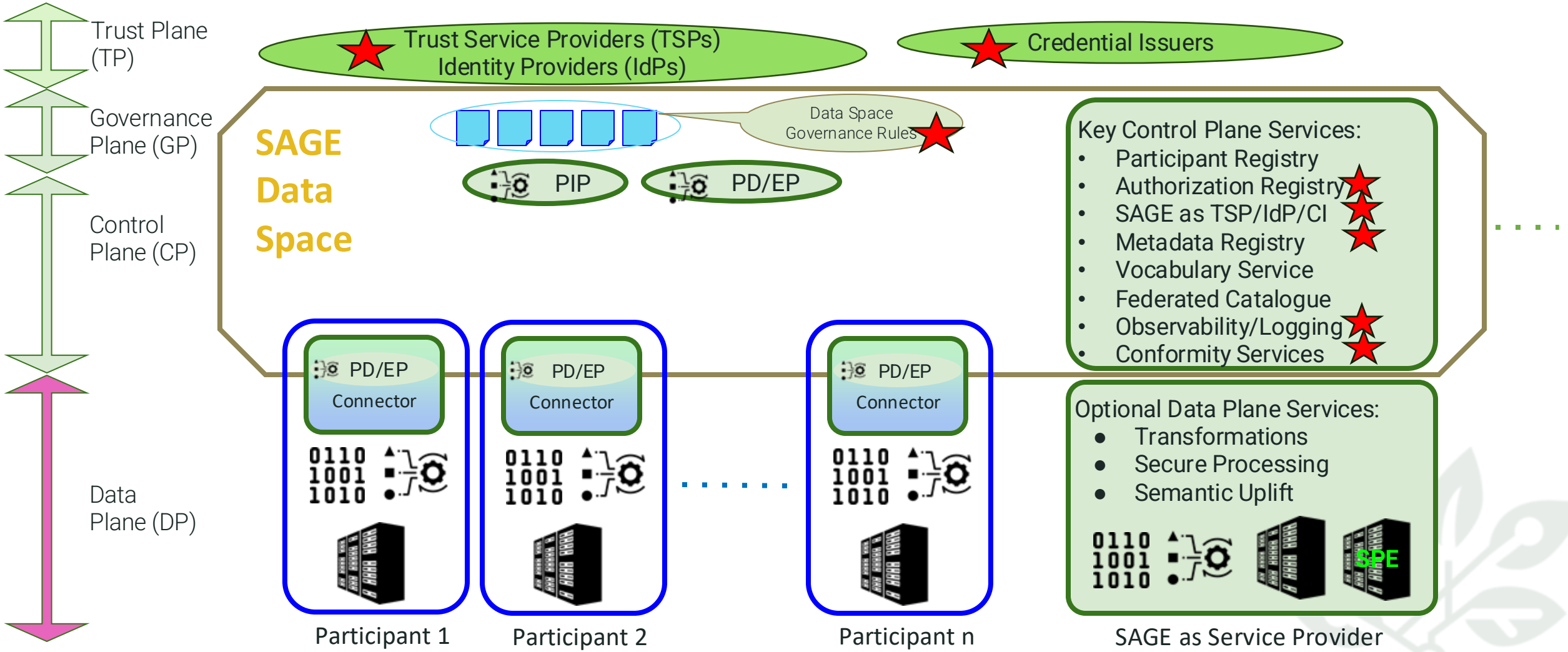
** Multi-layer reporting/governance using Data Sharing Groups*

- Sovereign data re-use through supply chain relationships
- Small as well as large participants through upcoming versions of Eclipse Dataspace Connector
- Semantic compliance with relevant metadata standards, enforced by data onboarding rules

Co-funded through the Digital Europe Programme (DIGITAL)
Grant agreement № 101195471

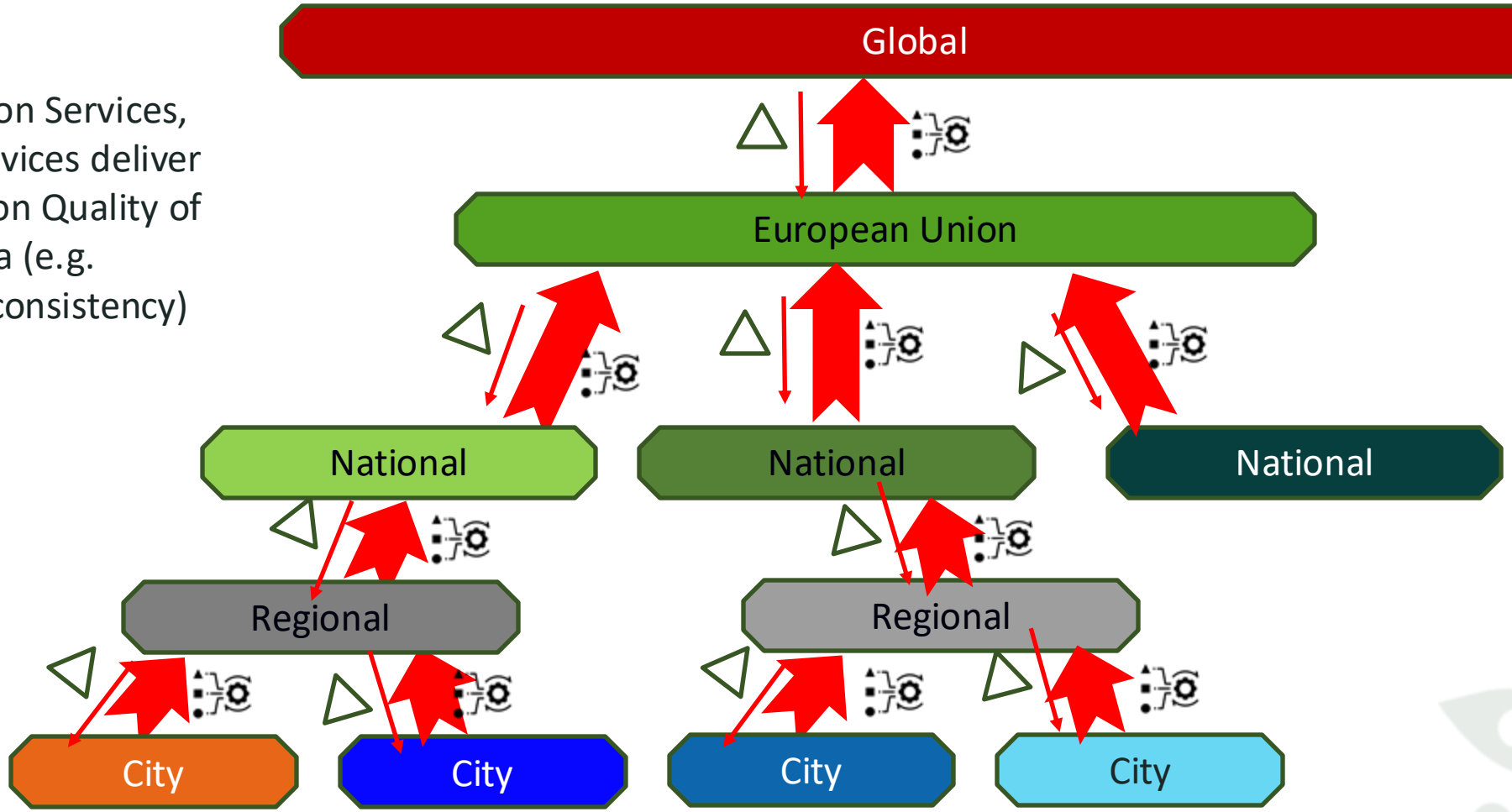
SAGE

Features of SAGE Supporting Reg Compliance



Multi-Layer Reporting

Transformation Services, Feedback services deliver Information on Quality of provided data (e.g. differences, consistency)



Trust Framework / Data Sovereignty in SAGE

TF/DS in SAGE starts with trusted, high assurance identity providers, such as eIDAS 1.0

- SAGE complements with other (external) IdPs: academic identities, corporate identities
- → consistent DID structure

Identities linked to Verified Certificates (e.g. ISO 27k certification for corporate IT, proof of house ownership for individual)

- Special purpose certificates to satisfy data visibility/access/re-use policies, e.g.
  - researchers need proof of training in handling of personal health information, before allowing access to such data
  - IT infrastructure must be proven to be a “secure processing environment” before transferring sensitive data there
  - Data consumer must be approved as not being a competitor of the data provider.

Connectors evaluate identities and credentials of data requesters against the rules of access for requested data (using ODRL)

Co-funded through the Digital Europe Programme (DIGITAL)
Grant agreement № 101195471

Extending Trust Framework for Compliance

Legal Trust Layer

- Qualified Trust Service Provider (QTSP)
- EU Trusted List
- Qualified Attestation of Attributes (QAA): Serves as the legal identity anchor for companies in wallet transactions.
- Qualified Signature / Seal: Enables organizations to sign Digital Declarations or documents, legally = to paper signatures.
- Legal Trust Chain: QTSP → QAA → Company (Holder) → Digital Declaration / VC → Verifier.
- Legal root of trust for environmental issuers (NFIs, certifiers, labs) participating in SAGE.

Operational Trust Layer

- Digital Declaration: legally valid for regulatory reporting (e.g. EUDR due-diligence statement, CSRD report). → B2G use.
- Digital Verifiable Credential (DVC): Non-qualified, W3C VC used for operational data exchange (e.g. product traceability, employee roles, audit proofs). → B2B or B2G use.
- Presentation / Selective Disclosure: Holder shares only required attributes per W3C Verifiable Credentials Data Model (VCDM). Ensuring privacy and minimal data exposure.

SAGE Integration:

- Issuers (e.g. NFIs, labs, certifiers) use their QAAs from QTSPs to anchor their credentials.
- SAGE issues DVCs for Green Deal use cases (Forestry, Textiles, CO_2 Hub).
- Digital Declarations handled through EUBW; DVCs handled through SAGE data space.

Result: Combined legal and operational trust layers create a future-proof architecture for Green Deal compliance.

Co-funded through the Digital Europe Programme (DIGITAL)
Grant agreement № 101195471

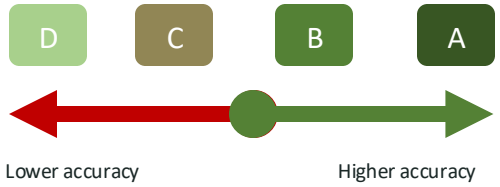
SAGE

Green Verified Credential Examples

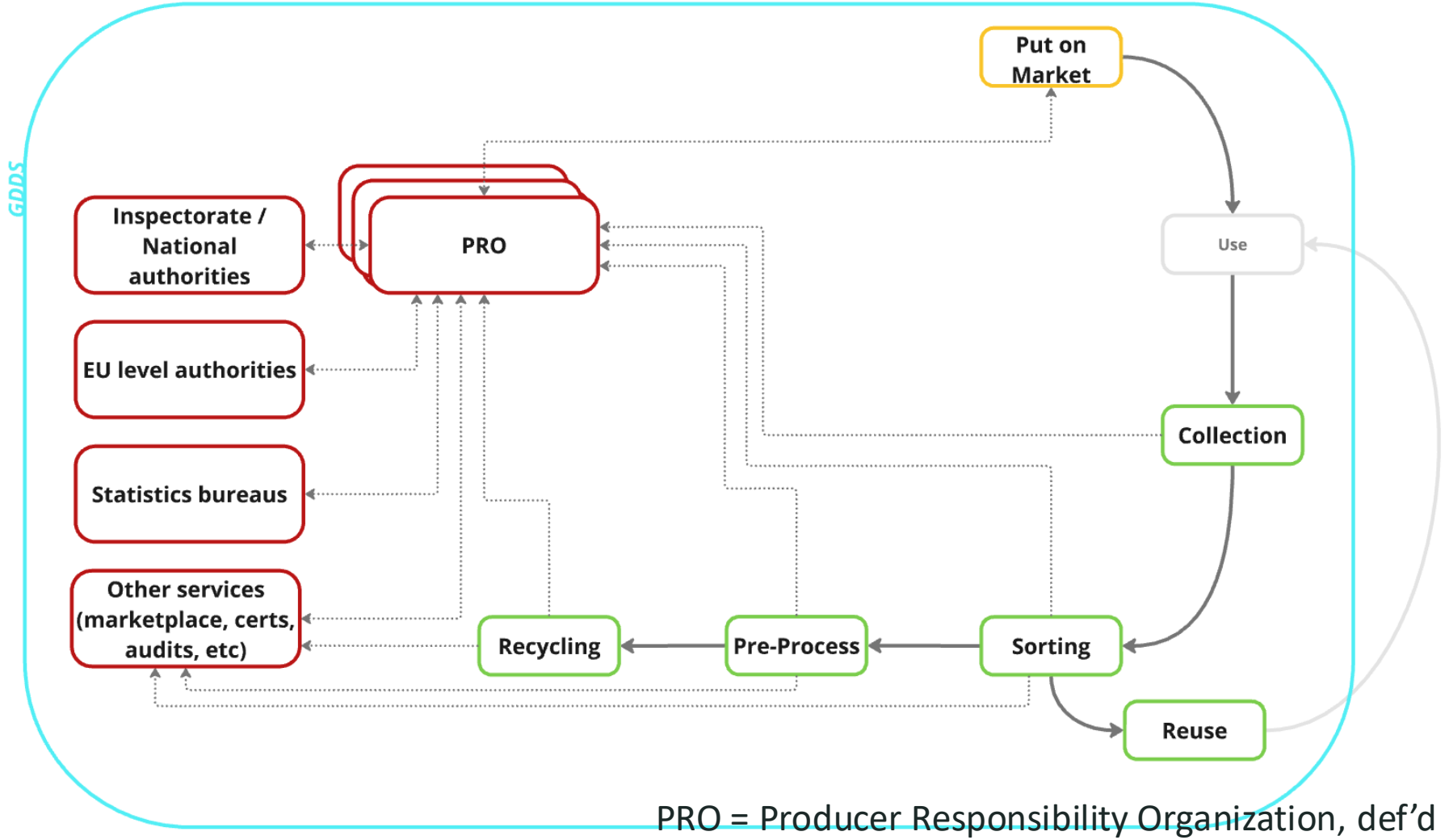
Use Case	Policy Basis	Credential Type	Example Template	Issuer	Verifier / Recipient
UC1: Forestry	EUDR	*Digital Declaration* (company-signed)	Due-Diligence Statement	Economic Operator using EUBW seal/signature	TRACES / Competent Authority
		Digital Verifiable Credential (DVC)	Forest Compliance VC	NFIs, FSC, PEFC	DG ENV / SAGE verifier
UC5: Textiles	ESPR / DPP	*DVC*	Recycled Material VC	PROs, Labs	Regulator / SAGE verifier
UC4: CO_2 Hub	CSRD	*Digital Declaration + DVC*	CO_2 Disclosure VC	Auditors / Companies	DG ENV / EBA

UC4: Standardized description of emission calculation methods enables comparison

General Calculation method:	Allocation: materials	Allocation: logistics	Materials Consumption data	Materials Emission factor	Logistics Method	Calculation method for other emissions		Verification
Maintenance area	A	A	A	A	A	A	Actuals-level	Yes Accredited
	B	B	B	B	B		Hybrid tai average - level	Yes Partially, Accredited
	C	C	C	C	C		Calculation based on itemised consumption in euros	Yes other
Company level			D	D			Calculation based on total consumption in euros	
							The sub-area was not calculated separately	No



UC5: Supply Chain Data Flows & Reporting



PRO = Producer Responsibility Organization, def'd in ESPR

SAGE

Conclusion

Baseline design of SAGE enables key aspects of robust regulatory compliance solution

- Robust trust framework/data sovereignty solution
- Multi-layer reporting/governance using Data Sharing Groups
- Sovereign data re-use across supply chain relationships
- Small as well as large participants through upcoming versions of Eclipse Dataspace Connector
- Semantic compliance with relevant metadata standards, enforced by data onboarding rules

Trust Framework can be extended specifically to support regulatory compliance – in alignment with plans for eIDAS2 and EUDI Wallets

Specific Certificate types can be defined to enable, e.g.:

- EUDR B2G declarations + B2B certifications
- ESPR/DPP traceability
- CSRD disclosures

Other Certificates can be defined as needed

Co-funded through the Digital Europe Programme (DIGITAL)
Grant agreement № 101195471

greendealdata.eu

SAGE Data Space

#

Mark Dietrich
Bloodstone Consulting Oü
Tallinn, Estonia

M: +351 (913 216 374)
mjdietrich@bloodstone-consulting.com

SAGE Technical Coordinator

Disclaimer: Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the Digital Europe Programme (DIGITAL). Neither the European Union nor the granting authority can be held responsible for them.

This project has received co-funding from the Digital Europe Programme (DIGITAL) under grant agreement № 101195471.