Digital product passport outlook under the ESPR

„Enabling digital product passport readiness “

Tim Schojohann (CEO Cryptar)

Digital product passport (DPP) as game changer for product standards*

Regulator

- Increase envionmental sustainability of products
- Encourage market surveillance authorities to step up digitalisation of product inspections and data collection
- Promote circularity by enabling new ecosystems through data (e.g.: refurbish, repair, recycle)

Manufacturer

- Better informed choices to increase product quality and sustainability
- Support the establishment of cross-sectoral value chains, opening up new markets
- Enable automated predictive and prescriptive resource efficiency strategies

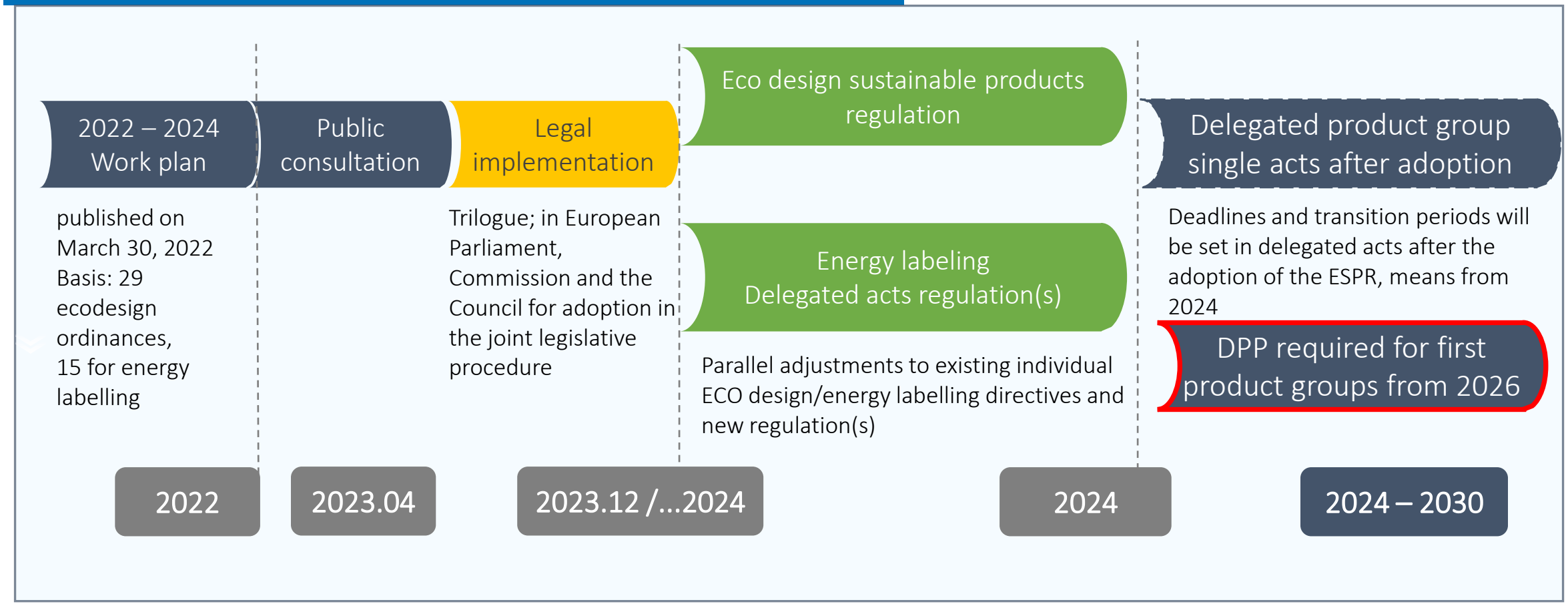
Consumer

- Better informed decisions by taking environmental impact into consideration
- Increase trust through transparency like repair guides, re-use, carbon footprint, lifecycle
- Protection from counterfeit or dangerous products

*https://circulareconomy.europa.eu/platform/sites/default/files/cisl_digital_products_passport_report_v6.pdf

Ecodesign Sustainability Products Regulation (ESPR) & DPP

Timing: 2023/2024



Digital product passport beyond buzzwords

A digital-based supply chain compliance tool, driven through product and consumer rights regulations

Article 2 definitions (29.)*

"product passport" means a **set of data specific to a product** that includes the information specified in the applicable delegated act adopted pursuant to Article 4 and that is **accessible via electronic means** through a data carrier in accordance with Chapter III;

Article 5 – Ecodesign requirements*

a) durability;
b) reliability;
c) reusability;
d) upgradability;
e) reparability;
f) possibility of maintenance and refurbishment;
g) presence of substances of concern;
h) energy use or energy efficiency;
i) resource use or resource efficiency;
j) recycled content;
k) possibility of remanufacturing and recycling;
l) possibility of recovery of materials;
m) environmental impacts, including carbon and environmental footprint;
n) expected generation of waste materials.

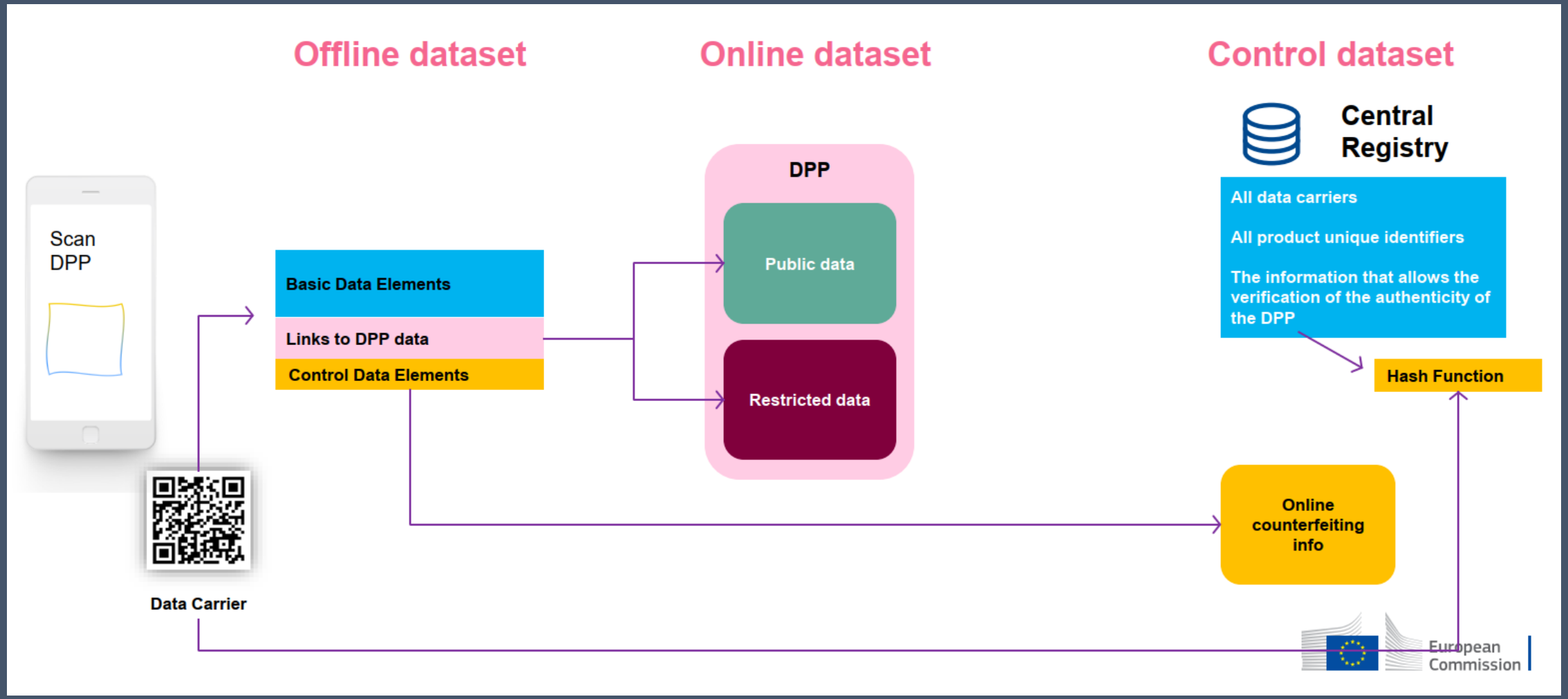
*https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2022:0142:FIN

TÜVRheinland®

cryptar

Current considerations for designing the digital product passport

accessible via electronic means through a data carrier in accordance with Chapter III



https://ec.europa.eu/docsroom/documents/54874/attachments/1/translations/en/renditions/native

What does this mean in practice?

Increased data governance requirements for DPP issuers

Authorized ecosystem partners & institution access

Publicly available to consumers

Restricted data

Technical File

- Material safety data sheet
- Bill of materials
- Declarations of Conformity (DoC) from manufacturer (ROHS, Toys directive, MD, LVD, EMCD, RED)
- Certificates of conformity from certification body (ROHS, Toys directive, MD, LVD, EMCD, RED)
- DoC for CE
- Third party test reports
- Third party test certificates (EU-type examinations, GS mark, type approval,….)
- . . .

DPP

Public data

Restricted data

Basic data elements

Public data

Sustainability performance;

- Repairability (repairability index)
  Repair guidance
- Durability declaration
- Recyclability (Content of recycled materials and degree of recycle design)
- Product carbon footprint
- Warranty
  → “green performance test report(s)”
  → “green performance certificate(s)”
- CE marking
- User manual
- . . .

Shared partial information

Shared partial information

TÜVRheinland®

cryptar

Status quo of product information provided in the industry

Regulator

- **27 % banned cotton** from chinese forced labour region despite regulation in the USA*[1]
- **40 %** of claims **have no supporting evidence***[4]

Manufacturer

- **9 % lost revenue** due to interorganisational fraud *[2]
- **79 %** of organisations **DO NOT share product data** with others as of 2022*[3]

Consumer

- **53 % of green claims give vague**, misleading or unfounded **information***[4]
- **75 % of consumers DO NOT trust** claims about environmental practices in the fast-moving consumer goods industry*[5]

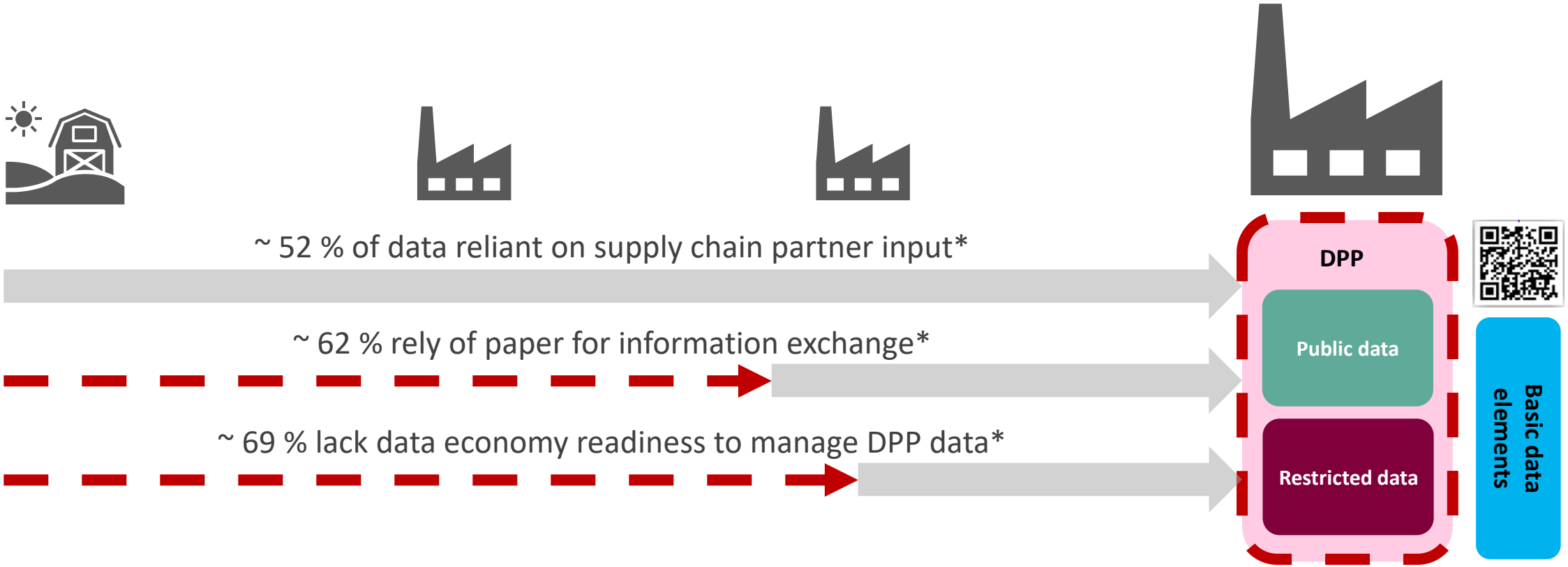
*[1] https://www.reuters.com/markets/commodities/us-customs-finds-garments-made-with-banned-chinese-cotton-documents-2023-09-01/,
*[2] https://ieeexplore.ieee.org/document/8948004,
* [3]BDI_IW-Report_2023-Digitaler-Produktpass,
*[4] https://environment.ec.europa.eu/topics/circular-economy/green-claims_en,
*[5] https://www.gfk.com/blog/greenwashing-brand-equity-how-to-bridge-the-trust-gap

TÜVRheinland®

cryptar

Manufacturers must ensure valid digital product passport entries to avoid fines and penalties

while lacking prerequisites across the supply chain for trusted information



*BDI_IW-Report_2023-Digitaler-Produktpass

Implications of status quo to digital product passport implementation

Regulator

- Official digital product passport documentation lacking foundation for content validation
- Limited technical enforcability due to „phygital“ setup with manual control mechanisms
- Focus on legal leverage with requirement to make an example of initial misbehaviour

Manufacturer

- Highly manual (and costly) but mission critical „phygital“ information governance and verification processes required
- High level of remaining 3rd party risk for brand reputation impacting sourcing strategies
- Requirement to proof sufficient risk mitigation efforts to avoid fines in case of legal disputes

Consumer

- Lack of justification for increased trust-level compared to current manufacturer trust seals
- „Informed decisions“ based on wealth of information provided rather than verified accuracy
- Reliance on sample testing and enforcement of policies drives public interest in making examples

TÜVRheinland®

cryptar

How to establish digital product passport ready information?

Foundation for control mechanisms and value creation beyond regulatory burden

Consistent data governance and data source validation needed

to manage accountability for digital product passport compliancy

Paper must become machine-readable and secured where it cannot be replaced

to protect against forgery and ensure information authenticity

Information integrity and authenticity verification should be automated

to scale without driving costs and risk through manual processes

TÜVRheinland®

cryptar

Establishing **trusted digital product passport documents**

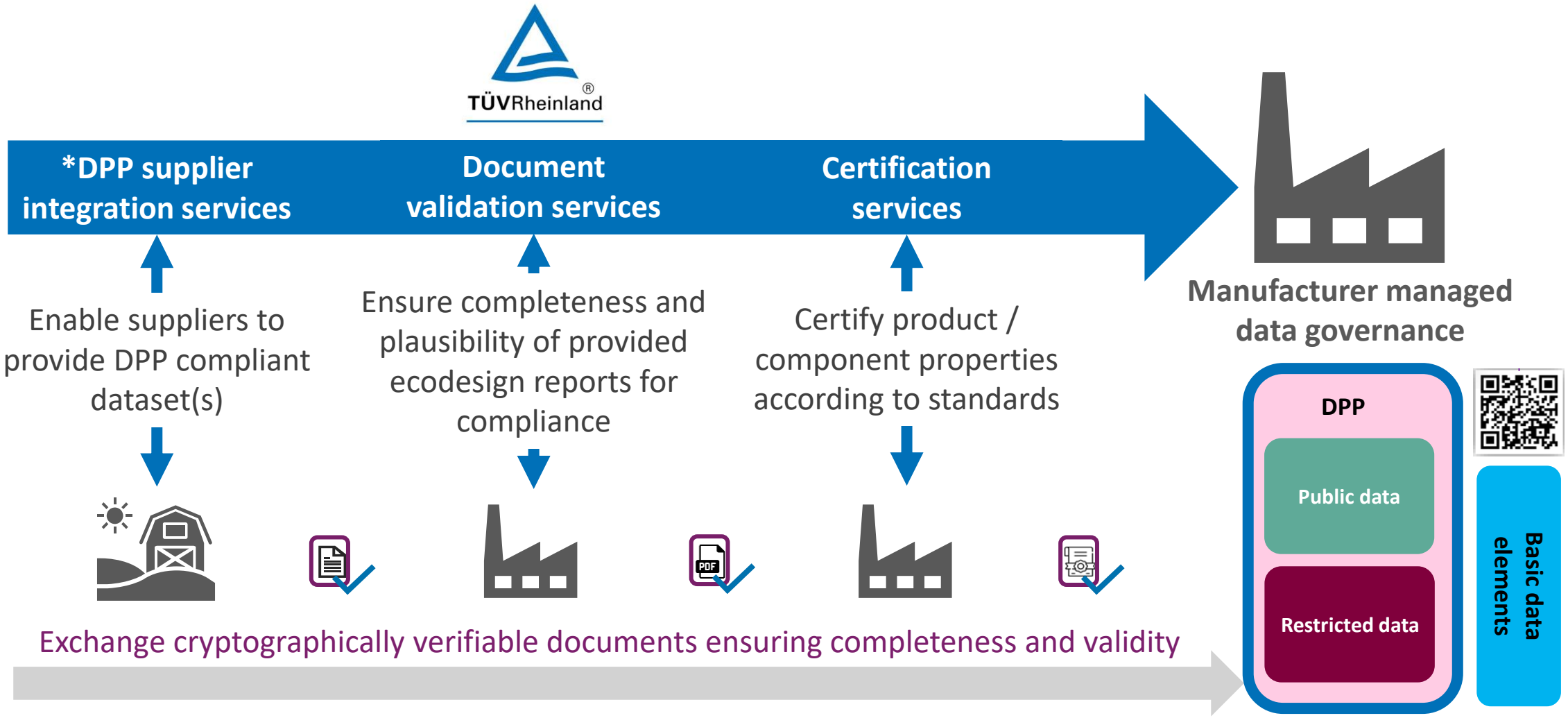
for entries with reduced 3rd party risk and automated compliance controls

- Officially recognized validator for product information
- Touches already a large percentage of documents in supply chains
- Deep expertise in regulations, standards and conformity requirements and assessments

Officially validated product data secured with **integrated validity controls**

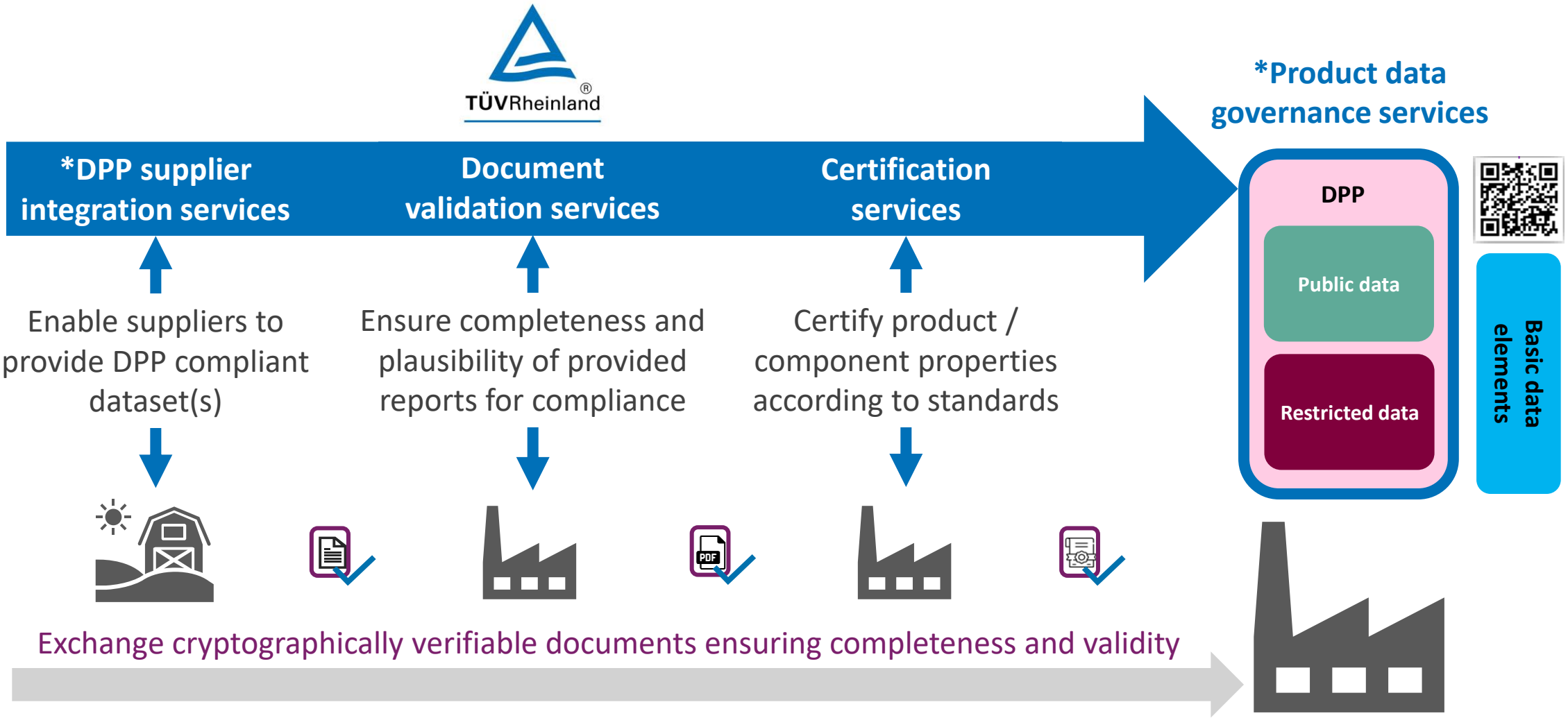
- Novel protocol for evidential cryptographic data lifecycle documentation
- Establishing trusted documents and datasets that
  - are tamper-proof
  - contain version control mechanisms
  - enable secure „phygital“ processes (machine-readable)
  - allow need-to-know sharing (partial data copies)
  - detect 3rd party signature abuse
  - enable integration of on- and offline validity checks
- Allowing infrastructure independent integration for validity controls across digital and „phygital“ processes

Service model considerations – information validity



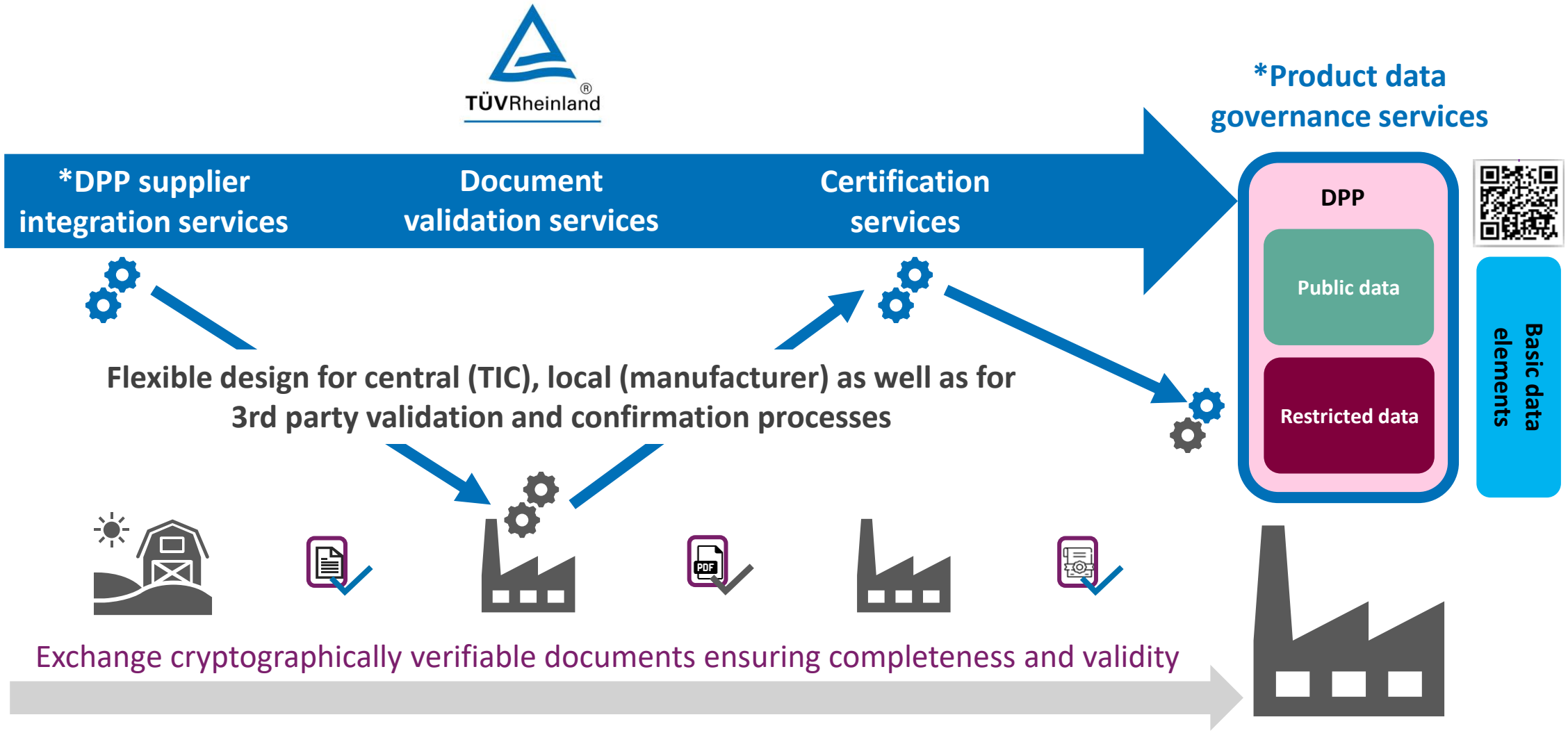
*Services to be established based on current customer process requirements

Service model considerations – data governance



*Services to be established based on current customer process requirements

Service model considerations – process integration



*Services to be established based on current customer process requirements

Advantages of verifiable digital product passport documents

Regulator

- Automated validity controls for critical product passport content through specialized TIC industry
- Understand origin of potential misinformation to address root-cause of dangerous products
- Focus on data patterns to remove fraudsters and enable synergies across sectors

Manufacturer

- Minimize costs through automated digital product passport compliancy verifications
- Leverage verified DPP documents and certified components to reduce 3rd party risk across supply chain
- Demonstrate certification and quality assurance efforts to consumers & authorities

Consumer

- Increase trust levels through transparent information sources and official certifications
- Informed decisions based on verified information accuracy
- Improved product safety through traceable certifications and automated validity controls

TÜVRheinland®

cryptar

Next steps for interested parties

Start & intro workshops (~ 2 hours)

- Discuss DPP requirements and proposed model in more detail
- Gain high level understanding of individual requirements

Initial deep dive workshops (~ 1 day)

- Establish understanding of required DPP contents
- Align on data governance requirements and own IT capabilites
- Discuss strategy for secure information gathering across supply chain

Initiative participation (limited availability – ongoing)

- Participate in product information focused jobs-to-be-done interviews
- Collaborate with TÜV Rheinland and Cryptar for integration requirements
- Shape final solution to meet individual requirements of your value chain

TÜVRheinland®

cryptar

Thank you

E-Mail: info@cryptar.de

Office phone: +49 (0) 89 1250 1227 1

Office address:
Leopoldstr. 102
80802 Munich
Germany