The European Metrology Cloud: Impact of European Regulations on Data Protection and the Free Flow of Non-Personal Data

Florian Thiel* and *Jan* Wetzlich

Physikalisch-Technische Bundesanstalt (PTB), 10587 Berlin, Germany

Abstract. New digital technologies, such as cloud computing, big data, artificial intelligence and the Internet of Things (IoT) are designed to maximize efficiency, enable economies of scale and develop new services. They offer benefits to users, such as agility, productivity, speed of deployment and autonomy. In the sector of Legal Metrology, it must be ensured that digital system architectures, digital services, and digital infrastructures are legally compatible. To benefit the stakeholders in this sector, the industry, the notified bodies and the market surveillance/verification authorities alike, the digital transformation of Legal Metrology shall remove barriers to innovation within the legal processes and reduce costs and time to market for new digital products. To this end a European consortium has formed to establish a digital quality infrastructure; the "European Metrology Cloud", designed to support the processes of conformity assessment and market surveillance/verification and the development of reference architectures and new technology- and data-driven services for this infrastructure. With this approach, the digital single market that the European Commission envisions will be fostered. This article analyzes how recent regulations within the digital single market strategy of the commission - the Data Protection Police Directive (2016/679/EU) and the Regulation on a framework for the free flow of non-personal data in the European Union (Regulation (EU) 2018/1807) – may be integrated into the European Metrology Cloud initiative to, e.g. guaranty that its underlying Blockchain approach complies to these norms and exploit their benefits.

1 Introduction

To foster the digital transformation in Legal Metrology, a pan European consortium led by PTB, Germany has initiated the development of a coordinated European digital quality infrastructure for innovative products and services; the “European Metrology Cloud” [1]. Its foundation lies in a metrological trust network formed by individual “nodes” located at the stakeholders in the member states. It is designed to support and streamline regulatory

processes by joining existing infrastructures and databases, and to provide a single-point-of-contact for all stakeholders. Within this quality infrastructure, reference architectures, i.e. innovative measuring instruments, as well as technology- and data-driven digital services for Legal Metrology will be developed. The results of the project's initial three years phase will serve as blueprints for the individual national plat-forms to attract and to integrate further European stakeholders and services and will support or even initiate processes for future-proof national and European legislation. With these objectives, the initiative fosters the European Commission's envisioned digital single market [2-11].
Several novel reforms and regulation proposals on the European level in the Commission's framework "Building a European Data Economy" might impose new requirements on or could solve open questions in this framework.

The **Data Protection Police Directive** (GDPR) [12] is part of the new EU's data protection rules adopted in April 2016 and applies since 25 May 2018 (Regulation (EU) 2016/679) [3]. The reform's main objective was to make the EU's data protection standards fit for the digital age and future-proof for technological developments. The Directive protects individuals when their personal data are processed by authorities for the purposes of prevention, investigation, detection or prosecution of criminal offenses or for the execution of criminal penalties. The rules deliver on the EU's Agenda on Security, the EU's strategy in the fight against terrorism, organized crime and cybercrime. The exchange of such data is essential in the fight against terrorism and cross border crime. Thanks to the new rules, sharing such data will be more efficient both at EU-level and international level. They will build trust and ensure legal certainty cross border.

The objective of the **Regulation on a framework for the free flow of non-personal data** in the European Union (Regulation (EU) 2018/1807) [13] is to achieve a more competitive and integrated EU market for data storage and/or processing services and activities. More specifically this means to reduce the number and range of data localization restrictions, enhance legal certainty; facilitate cross-border availability of data for regulatory control purposes; improve the conditions under which users can switch data storage and/or processing service providers or port their data back to their own IT systems; enhance trust in and the security of cross-border data storage and/or processing [14, 15].

This article aims at analyzing how the regulatory requirements of the Data Protection Police Directive (2016/679/EU) and of the Regulation on a framework for the free flow of non-personal data in the European Union (Regulation (EU) 2018/1807) may impact on and in which way they could be integrated into the European Metrology Cloud initiative to guaranty compliance to these norms.

The remainder of this paper is structured as follows:

1. The European Metrology Cloud conceptional fundament is explained.
2. The specifics of the General Data Protection Regulation and the Regulation on a framework for the free flow of non-personal data are summarized.
3. The Impact of both regulations on the European Metrology Cloud is investigated, focusing especially on the underlying Blockchain approach.
4. The last section gives an overview of the results.

2 The European Metrology Cloud

2.1. Objectives: Join Infrastructure and databases

To reduce the administrative burdens for businesses, and to expedite and harmonize the administrative process of conformity assessment and market surveillance, a digital quality infrastructure for European Legal Metrology needs to be developed that aggregates existing IT infrastructures and databases of the partners (Industry, Notified Bodies and Market Surveillance) towards a Legal Metrology Grid [1] (s. figure 1).

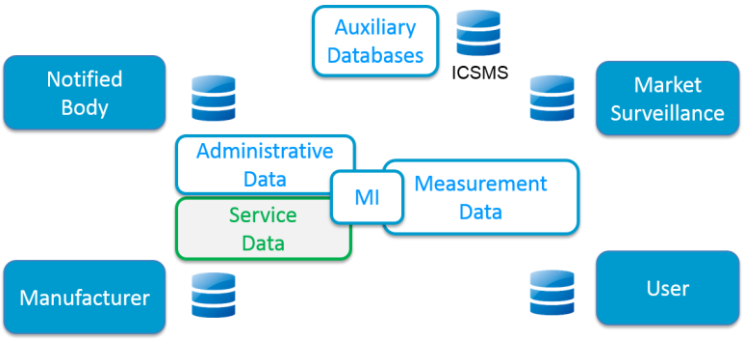

Fig. 1. Stakeholders in Legal Metrology and their main Data sources. Three Data classes can be distinguished related to the measuring instrument (MI) [1].

For the interoperable interconnection of infrastructures and databases, a secure and trustworthy platform needs to be established (s. figure 2), e.g. in every member state. A blueprint for the member states' platforms will be developed which serves as a communication and service platform and a single-point-of-contact [1].

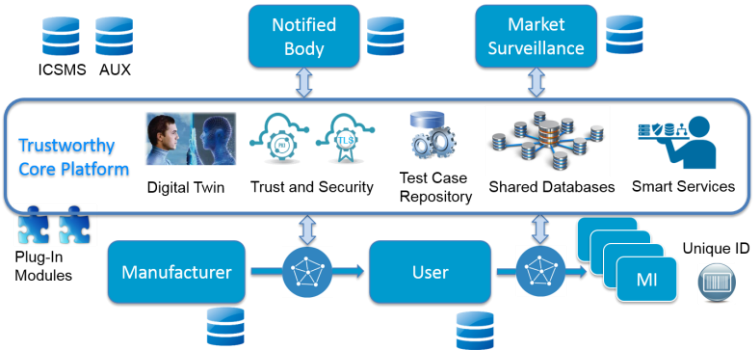

Fig. 2. Concept of the trustworthy platform and it's elements [1].

The term cloud can cause considerable confusion as it has many connotations. This may originate from the most common interpretation of a "Cloud" as a virtual place for dumping data, e.g. on a server in an adequate data center. Setting up a facility for storing data, is not in line with the aims of the European industry, e.g. because of the tremendous cost for extra security to prevent this "honey pot" of sensitive data from being hacked. Let alone that no industry partner will place data that contain intellectual property in a structure that might be hosted or developed by a potential concurrent, e.g. MindSphere. Besides that, the Cloud can provide Infrastructure-, platform- or software as a service and, hence, can also be put into practice in the form of a distributed network of nodes that provide data and access to them

[17]. We, therefore, interpret the term "Cloud" as a synonym for the trusted metrological core platform which is a distributed, node-based system. We like to emphasize here, that, due to security reasons, the storage of data related to the measuring instrument in that network will be reduced to an absolute minimum. We will concentrate on administrative and service data which are used in processes. To guaranty data sovereignty by design, data will be made available via the authorized access to databases under the control of the individual stakeholders via an individual node (s. figure 3).

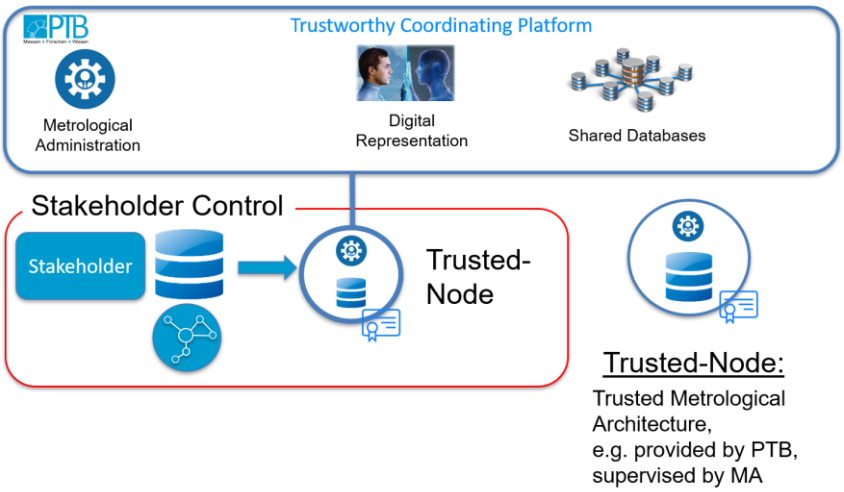

Fig. 3. Node-Concept of the trustworthy platform to guaranty Data Sovereignty by Design [1, 16]. MA: Market Surveillance / Verification Authority.

The design options and decisions which lead to this concept are summarized in [17].

2.2. Main Impact

The main impact of this digital quality infrastructure is manifolded and will be listed in the following:

- The establishment of a Metrological Trust Anchor
- The easy Integration of Contributors, Data, and Infrastructures
- Digitally rendered Workflows
- Digitally Streamlined Metrological Processes
- Harmonization of processes by Technology
- The possibility to repair/verify a large number of measuring instruments remotely
- Such digital support services reduce the downtime of the measuring instrument.
- Globally available measuring instrument data (Manuals, Certificates, etc.)
- Open to integrate concepts from other regulated areas.
- Open to integrate other trust-based workflows

More details are explained in [1].

2.3. Nature of the Data

Within the legal framework of Legal Metrology, a multitude of processes are defined and well established in a certain way, applying traditional communication paths. These processes range from the exchange of information between partners, such as the documentation of the instrument design provided by the manufacturer during the assessment of conformity at the notified body, between the market surveillance and the manufacturer when the instrument is put into use or during the re-verification phase between the manufacturer and the verification authorities after the repair of an instrument. The interaction within these processes is currently not based on state-of-the-art communication paths or coordinated via platforms. Furthermore, an obligation to collect specific data for the instruments for each role in this context is set up. The notified body maintains, for example, a database of the tests during conformity assessments and documentation of all the individual instruments carried out by them. This is highly sensitive information. Another example is the performance data of a measuring instrument. Manufacturers shall carry out sample testing of measuring instruments made available on the market, investigate and maintain a register of complaints of non-conforming measuring instruments and measuring instrument recalls, and shall keep distributors informed of any such monitoring. Data that the market surveillance authorities shall collect are, for example, the data necessary for the identification of non-compliant measuring instruments, the origin of the measuring instrument, the nature of the alleged non-compliance and the risk involved, the nature and duration of the national measures taken, and the arguments put forward by the relevant economic operator. Retrieving data from metrology databases is done on request in traditional ways based on queries carried out by the keeper of the database as an intermediator and transferred back by this role to the requestor. Direct queries by an authorized partner to data provided by the partners are not yet possible. There are several processes in place where many different partners are involved, and their agreement is needed based on different actions that must be carried out before a final process can be initiated. A prominent example is the change, repair or update of legally relevant software. There are good prospects to streamline such processes if rendered digitally via a platform and blockchain based Smart Contracts [1].

All stakeholders are legal entities and the data which are processed within the legal processes are related to a single or a type of measuring instrument.

3 General Data Protection Regulation

3.1. Objectives

The aim of the GDPR is to protect all EU citizens from privacy and data breaches in today's data-driven world. Although the key principles of data privacy still hold true to the previous directive, many changes have been proposed to the regulatory policies; the key points of the GDPR, as well as information on the impacts it will have on business, can be found below.

3.2. Definition of Terms

In the following, the definition of a few relevant terms will be given [12].

- **Personal data** means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors

specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

- **Processing** means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
- **Controller** means the natural or legal person, public authority, agency or another body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;
- **Processor** means a natural or legal person, public authority, agency or another body which processes personal data on behalf of the controller;
- **Consent** of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by clear affirmative action, signifies agreement to the processing of personal data relating to him or her;
- **Personal data breach** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed;

3.3. Territorial Scope

The biggest change to the regulatory landscape of data privacy comes with the extended jurisdiction of the GDPR, as it applies to all companies processing the personal data of data subjects residing in the Union, regardless of the company's location. Previously, territorial applicability of the directive was ambiguous and referred to the data process 'in the context of an establishment'. This topic has arisen in a number of high-profile court cases. GDPR makes its applicability very clear – it applies to the processing of personal data by controllers and processors in the EU, regardless of whether the processing takes place in the EU or not. The GDPR also applies to the processing of personal data of data subjects in the EU by a controller or processor not established in the EU, where the activities relate to: offering goods or services to EU citizens (irrespective of whether payment is required) and the monitoring of behavior that takes place within the EU. Non-EU businesses processing the data of EU citizens also have to appoint a representative in the EU.

3.4. Penalties

Organizations in breach of GDPR can be fined up to 4% of annual global turnover or €20 Million (whichever is greater). This is the maximum fine that can be imposed for the most serious infringements e.g. not having sufficient customer consent to process data or violating the core of Privacy by Design concepts. There is a tiered approach to fines e.g. a company can be fined 2% for not having their records in order (article 28), not notifying the supervising authority and data subject about a breach or not conducting an impact assessment. It is important to note that these rules apply to both controllers and processors – meaning 'clouds' are not exempt from GDPR enforcement.

3.5. Consent

The conditions for consent have been strengthened, and companies are no longer able to use long illegible terms and conditions full of legalese. The request for consent must be given in an intelligible and easily accessible form, with the purpose for data processing attached to that consent. Consent must be clear and distinguishable from other matters and provided in an intelligible and easily accessible form, using clear and plain language. It must be as easy to withdraw consent as it is to give it.

3.6. Data Subject Rights

Breach Notification:

Under the GDPR, breach notifications are now mandatory in all member states where a data breach is likely to "result in a risk for the rights and freedoms of individuals". This must be done within 72 hours of first having become aware of the breach. Data processors are also required to notify their customers, the controllers, "without undue delay" after first becoming aware of a data breach.

Right to Access:

Part of the expanded rights of data subjects outlined by the GDPR is the right for data subjects to obtain confirmation from the data controller as to whether or not personal data concerning them is being processed, where and for what purpose. Further, the controller shall provide a copy of the personal data, free of charge, in an electronic format. This change is a dramatic shift to data transparency and empowerment of data subjects.

Right to be Forgotten:

Also known as Data Erasure, the right to be forgotten entitles the data subject to have the data controller erase his/her personal data, cease further dissemination of the data, and potentially have third parties halt processing of the data. The conditions for erasure, as outlined in article 17, include the data no longer being relevant to original purposes for processing, or a data subject withdrawing consent. It should also be noted that this right requires controllers to compare the subjects' rights to "the public interest in the availability of the data" when considering such requests.

Data Portability:

GDPR introduces data portability – the right for a data subject to receive the personal data concerning them – which they have previously provided in a 'commonly use and machine-readable format' and have the right to transmit that data to another controller.

Privacy by Design:

Privacy by design as a concept has existed for years, but it is only just becoming part of a legal requirement with the GDPR. At its core, privacy by design calls for the inclusion of data protection from the onset of the designing of systems, rather than an addition. More specifically, '*The controller shall… implement appropriate technical and organizational measures… in an effective way… in order to meet the requirements of this Regulation and protect the rights of data subjects*'. Article 23 calls for controllers to hold and process only the data absolutely necessary for the completion of its duties (data minimization), as well as limiting the access to personal data to those needing to act out the processing.

Data Protection Officers:

Under GDPR it is not necessary to submit notifications/registrations to each local Data Processing Agreement (DPA) of data processing activities, nor is it a requirement to notify/obtain approval for transfers based on the Model Contract Clauses (MCCs). Instead, there are internal recordkeeping requirements, as further explained below, and DPO appointment is mandatory only for those controllers and processors whose core activities consist of processing operations which require regular and systematic monitoring of data subjects on a large scale or of special categories of data or data relating to criminal convictions and offenses. Importantly, the Data Protection Officer:

- Must be appointed on the basis of professional qualities and, in particular, expert knowledge on data protection law and practices
- Maybe a staff member or an external service provider
- Contact details must be provided to the relevant DPA
- Must be provided with appropriate resources to carry out their tasks and maintain their expert knowledge
- Must report directly to the highest level of management
- Must not carry out any other tasks that could result in a conflict of interest.

4 Free Flow of Non-Personal Data

New digital technologies, such as cloud computing, big data, artificial intelligence and the Internet of Things (IoT) are designed to maximize efficiency, enable economies of scale and develop new services. They offer benefits to users, such as agility, productivity, speed of deployment and autonomy. The free flow of non-personal data is a pre-requisite for a competitive data economy within the Digital Single Market. To fully unleash the data economy benefits we need to ensure a free flow of data, allowing companies and public administrations to store and process non-personal data wherever they choose in the EU. For instance, guidance on private sector data sharing has already been published by the Commission [13].

4.1. Objectives

Our economy depends more and more on data: data can create significant added value to existing services and facilitate entirely new business models. As estimated by one of the support studies, taking away obstacles to data mobility is expected to generate additional growth of up to 4% GDP by 2020 (Deloitte).

As indicated in the 2017 Communication "Building a European Data Economy", the value of the EU data market was estimated in 2016 at almost EUR 60 billion, showing a growth of 9.5% compared to 2015. According to a study, the EU data market could potentially amount to more than EUR 106 billion in 2020.

That is why the Commission has proposed to remove all disproportionate restrictions to the movement of data across the Member States and IT systems in Europe.
The Commission's work on the free flow of data was announced in the context of actions to enhance the data economy - see Communication "Building a European Data Economy" (10

January 2017), in a more targeted context, in the Communication "DSM mid-term review" (10 May 2017). The Regulation on the free flow of non-personal data is one of the sixteen intended actions listed in the Digital Single Market strategy of May 2015 [15].

To unlock this potential, the Regulation aims to address the following issues [15]:

- Improving the mobility of non-personal data across borders in the single market, which is limited today in many Member States by localization restrictions or legal uncertainty in the market;
- Ensuring that the powers of competent authorities to request and receive access to data for regulatory control purposes, such as for inspection and audit, remain unaffected; and
- Making it easier for professional users of data storage or other processing services to switch service providers and to port data, while not creating an excessive burden on service providers or distorting the market.

4.2. Definition of Terms

In the following, the definition of a few relevant terms will be given [15].

- **Data** means data **other than personal data** as referred to in Article 4(1) of Regulation (EU) 2016/679;
- **Data storage** means any storage of data in electronic format;
- **Provider** means a natural or legal person who provides data storage or other processing services;
- **Data localization requirement** means any obligation, prohibition, condition, limit or other requirement provided for in the laws, regulations or administrative provisions of the Member States, which imposes the location of data storage or other processing in the territory of a specific Member State or hinders storage or other processing of data in any other Member State;
- **Competent authority** means an authority of a Member State that has the power to obtain access to data stored or processed by a natural or legal person for the performance of its official duties, as provided for by national or Union law;
- **User** means a natural or legal person using or requesting a data storage or other processing service;
- **Professional user** means a natural or legal person, including a public sector entity, using or requesting a data storage or other processing service for purposes related to its trade, business, craft, profession or task.

4.3. Obstacles to Free Flow of Data

Today, the main obstacles that preclude the free flow of data in the Digital Single Market are [15]:

- Unjustified data localization restrictions by Member States' public authorities,
- Legal uncertainty about legislation applicable to cross-border data storage and processing,
- A lack of trust in cross-border data storage and processing linked to concerns amongst Member States' authorities about the availability of data for regulatory scrutiny purposes

- Difficulties in switching service providers (such as cloud) due to vendor lock-in practices.

4.4. New Regulation

The new Regulation will ensure:

- Free movement of non-personal data across borders: every organization should be able to store and process data anywhere in the European Union,
- The availability of data for regulatory control: public authorities will retain access to data, also when it is located in another Member State or when it is stored or processed in the cloud,
- Easier switching of cloud service providers for professional users. The Commission has started facilitating self-regulation in this area, encouraging providers to develop codes of conduct regarding the conditions under which users can port data between cloud service providers and back into their own IT environments,
- Full consistency and synergies with the cybersecurity package, and clarification that any security requirements that already apply to businesses storing and processing data will continue to do so when they store or process data across borders in the EU or in the cloud.

5 Impact Analysis

In our impact analysis, we are focusing on the Blockchain approach which we have in mind for certain trust elements in the Metrology Cloud.

In short Blockchain technology is characterized by a continuously growing number of data sets, which are chained by cryptographic methods. Later entries build on and confirm as correct on previous entries, which is why previous entries as such must remain unchanged, thereby at the same time making data manipulation more difficult. The Commission is of the opinion that the use of Blockchain in the digitization of trade has the potential to simplify and improve the work of customs authorities, increase the efficiency, speed and volume of global trade, and bring more benefits to the different actors [19]. It could create economic opportunities for Small and Medium Enterprises to internationalize and to overcome the costs associated with exporting. The European Parliament has recently approved a report “Blockchain: a forward-looking trade policy” which explains in detail the advantages and challenges associated with the use of Blockchain in international trade [18].

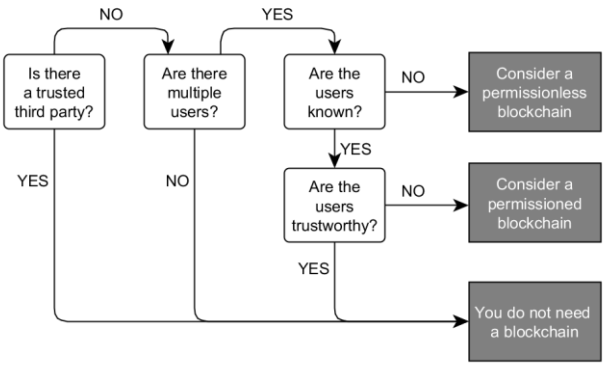

Fig. 4. Blockchain consideration for the European Metrology Cloud adapted from K. Wüst and A. Gervais, „Do you need a blockchain?“ In: Cryptology ePrint Archive, 2017/375.

To answer the question whether or not a Blockchain is needed for the Metrology Cloud or if a standard database is sufficient, the schema provided by Wüst and Gervais [20] could be applied (s. figure 4).

The answers resulting from this schema in figure 4 regarding the Metrology Cloud are the following:

Is there a trusted third party? – No

Are there multiple users? – Yes

Are the users known?- Yes

Are the users trustworthy – No

Resulting in the proposal to consider a permissioned Blockchain approach!

That’s why the decentralized ID Administration (PKI), the immutable logbook for process relevant data and the digitally transformed legal processes by Smart Contracts will be rendered by Distributed Ledger Technologies, e.g. the Blockchain in the Metrology Cloud (s. figure 5).

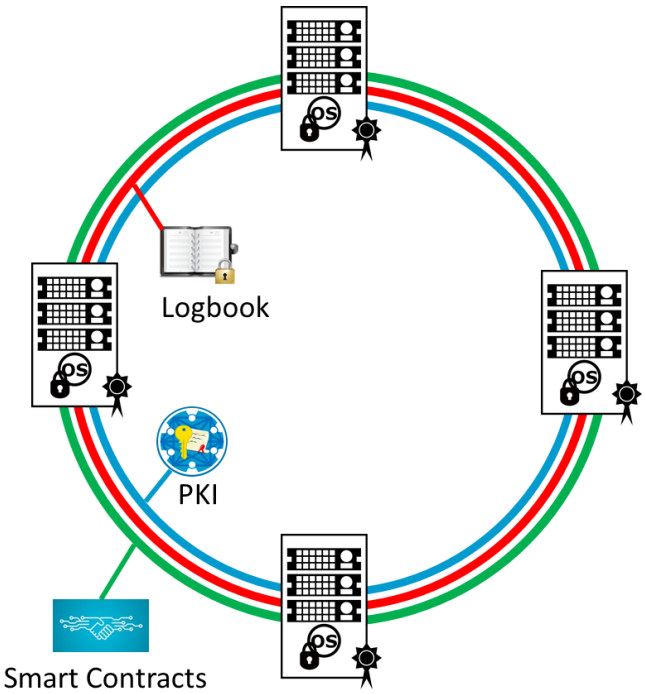

Fig. 5. Exemplary Metrology Cloud trust network with four nodes. The decentralized ID Administration (PKI), the immutable logbook for process relevant data and the digitally transformed legal processes by Smart Contracts will be rendered by Distributed Ledger Technologies, e.g. the Blockchain [21, 22].

5.1. Impact of General Data Protection Regulation

The Commission is looking into different challenges for the deployment of Blockchain, including the one related to compliance to EU laws. Regarding Blockchain and the General Data Protection Regulation (GDPR), the European Union Blockchain Observatory and Forum has recently issued a report [23] which analyses in detail the different possible elements of tension between the technology and the GDPR and attempts to provide different solutions to solve them. With respect to security issues, though any IT system can be subject to attacks, one could argue that permissioned (private) Blockchains are likely to be more robust, difficult to attack and resilient than central database systems. On the subject of energy consumption, though it is still a burning issue for permissionless systems such as Bitcoin and Ethereum, in permissioned distributed ledgers, the consensus mechanisms are automatically executed, and hence much more energy-efficient.

The Commission continues to monitor whether the legal framework is sufficient to allow the further beneficial development of blockchain technology and its applications in the EU [19].

One result of the former mentioned investigation is, that the blockchain technology seems to be in conflict with the principles of the European General Data Protection Regulation (GDPR), such as the principle of data minimization (Article 5 (1) (c) GDPR) and the right

to be deleted or the right to be forgotten (Article 5 and Article 17 GDPR) if personal data is stored in the blockchain.
As a matter of principle, these current legal frameworks will also have to be taken into account within the framework of Article 25 of the GDPR (privacy by design). It is assumed that providers and developers of innovative digital technologies are aware of these and other provisions of the GDPR and are sufficiently taken into account in the development of applications.

Since there is no such thing as GDPR-compliant blockchain technology, there are only GDPR-compliant use cases and applications [23].
Depending on the use cases there are different approaches for storing personal data GDPR-compliantly on a blockchain. Minimalistic approaches are e.g. making data unreadable by using encryption or storing only HMACs (hash of a concatenation of data plus a secret) in the chain. Only the data owner or Controller can than provide access to the data by providing the encryption key or proof that certain data is stored in the chain by providing the secret.
Zero-Knowledge-Proofs (ZKP) [24] also can provide privacy while still providing possibility to proof a claim. To do so only the proof is stored in the Blockchain, the proof itself does not contain any secret information. ZKP are a mathematical way to proof someone has some secret knowledge without disclosing this knowledge.
A more complex way would be to delete whole blocks from the chain while still pretending the integrity of the whole chain. For the Metrology Cloud the first proposal will be the fastest way. Nonetheless, the two other ways are also considered very promising. Therefore, we will also invest ongoing research into these solutions, too.

5.2. Impact of Free Flow of Non-Personal Data Regulation

Non-Personal data generated, processed and exchanged in the metrology cloud:

Part of the instrument generating data / storing data in another country.
Node concept facilitates the issues which the new regulation likes to address, like

- Free movement of non-personal data across borders: every organization should be able to store and process data anywhere in the European Union,
  - ⇨ Each participant in the EMC-network provides the data for the other permissioned participants, regardless of its localization in the EU.
- The availability of data for regulatory control: public authorities will retain access to data, also when it is located in another Member State or when it is stored or processed in the cloud,
  - ⇨ Each permissioned participant in the EMC-network has access to the data he or she is allowed to access, regardless where the node is located.

6 Conclusion

Regarding the GDPR it was recommended by [19] to avoid storing personal data on a blockchain. Instead make full use of data obfuscation, encryption and aggregation techniques in order to anonymize data to collect personal data off-chain or, if the blockchain can’t be avoided, on private permissioned blockchain networks. So, personal

data should be carefully considered when connecting private blockchains with a public one. This recommendation is fulfilled by our Metrology Cloud approach, for we are applying a permissioned blockchain.

All stakeholders within the Metrology Cloud are legal entities or legally defined roles, and the data which are processed within the legal processes are related to a single measuring instrument or a type of measuring instrument. Each instrument is identifiable by an unique identifier and not by data related to its user or the household it is located.

Even that it seems clear that in the current concept of the Metrology Cloud no personal data are processed, the right to be deleted or the right to be forgotten, should be incorporated in the Blockchain concept. In that way the system becomes GDPR ready and potentially usable to process personal data compliantly. Hence, on the one hand minimalistic approaches like making data unreadable by the data owner will be integrated and on the other hand new concepts for deleting a single entry or chains of entries by a legitimated authority will be developed and integrated. In that way, the concept “privacy by design” is also addressed.

The requirement of data minimization is inherent in the metrology cloud concept, since the data needed within the individual legal process are already defined. Regarding the Free Flow of Non-Personal Data Regulation, it can be concluded that the Node concept of the Metrology Cloud already facilitates the issues which the new regulation likes to facilitate.

So, it can be concluded that the Metrology Cloud benefits from these new regulations making it future proof and even more in line with the digital market strategy of the European Commission.

Acknowledgements

This research was carried out within the framework of the project “AnGeWaNt” [25], which focuses - amongst others - on an exemplary implementation of the Metrology Cloud’s concept for the specific needs of a selected class of measuring instruments, the weighing instruments. The project AnGeWaNt is funded by Germany’s Federal Ministry of Education and Research (BMBF) and the European Social Fund (ESF) as part of the "Future of Work: Work in Hybrid Value Creation Systems" program and supervised by the project sponsor Karlsruhe (PTKA) (Funding Code: 02L17B050).

References

1. F. Thiel: "Digital transformation of legal metrology - The European Metrology Cloud", OIML Bulletin, vol. LIX, 2018(1), pp. 10-21
2. Digital Single Market, Bringing down barriers to unlock online opportunities, European Commission, Priorities, https://ec.europa.eu/priorities/digital-single-market_en, (retrieved: 2017-02-21)
3. A vision for the internal market for industrial products, European Commission, COM (2014) 25 final, http://cor.europa.eu/en/activities/stakeholders/Documents/Com%202014-25.pdf, (retrieved: 2017-02-21)
4. P. Cloutier, J. Meurer, CECOD vision of “new Big Data World” with metrology constraints, PTB - Mitteilungen, 1/2017, page 7-8, doi: 10.7795/310.20170199

5. I. Turner, Recent Software Developments – The view of the weighing industry, PTB -Mitteilungen, 1/2017, page 3-6, doi: 10.7795/310.20170199
6. Data economy strategy, European Commission, https://ec.europa.eu/digital-single-market/en/towards-thriving-data-driven-economy, (retrieved: 2017-02-21)
7. Cloud Computing, European Commission, https://ec.europa.eu/digital-single-market/en/cloud, (retrieved: 2017-02-21)
8. Digital Single Market – Digitizing European Industry Questions & Answers, European Commission - Fact Sheet, http://europa.eu/rapid/press-release_MEMO-16-1409_en.htm, (retrieved: 2017-02-21)
9. Towards a thriving data-driven economy, European Commission COM (2014) 442 final http://ec.europa.eu/newsroom/dae/document.cfm?action=display&doc_id=6210 (retrieved: 2017-02-21)
10. Legal Metrology, European Commission, http://ec.europa.eu/growth/single-market/goods/building-blocks/legal-metrology/, (retrieved: 2017-02-21)
11. Key Issues for digital Transformation in the G20, Report prepared for a joint G20 German Presidency / OECD conference, OECD (2017), http://www.bmwi.de/Redaktion/DE/Downloads/G/g20-key-issues.html, (retrieved: 2017-02-21)
12. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
13. Regulation (EU) 2018/1807 on a framework for the free flow of non-personal data in the European Union
14. European Commission, Guidance on private sector data sharing, https://ec.europa.eu/digital-single-market/en/guidance-private-sector-data-sharing
15. European Commission, Free flow of non-personal data, https://ec.europa.eu/digital-single-market/en/free-flow-non-personal-data
16. Dohlus M. , Nischwitz M., Yurchenko A., Wetzlich J., Integrated Information Systems: Design-Options for Consortial Plattforms, PTB-Metrology-Cloud Whitepaper 2018, available here: https://www.ptb.de/cms/fileadmin/internet/fachabteilungen/abteilung_8/8.5_metrologische_informationstechnik/181213_Whitepaper_Design_Ops_Metrology_Cloud.pdf
17. F. Thiel, M. Esche, D. Peters, U. Grottker; "Cloud Computing in Legal Metrology", 17th International Congress of Metrology, 16001 (2015), DOI:10.1051/metrology/201516001, EDP Sciences (2015)
18. European Parliament, Report on Blockchain: a forward-looking trade policy (2018/2085(INI)), http://www.europarl.europa.eu/doceo/document/A-8-2018-0407_EN.html
19. EN E-006338/2018 Answer given by Ms Gabriel on behalf of the European Commission (15.3.2019) http://www.europarl.europa.eu/doceo/document/E-8-2018-006338-ASW_EN.pdf
20. K. Wüst and A. Gervais, „Do you need a blockchain?" In: Cryptology ePrint Archive, 2017/375, https://eprint.iacr.org/2017/375.pdf
21. Wetzlich J, Nischwitz M, Thiel F, Seifert J.-P., A Modular Testbed for Intelligent Meters and their Ecosystem, FedCSIS 2017, ACSIS, Vol. 13, pp. 119–125, DOI: 10.15439/2017F556, ISSN 2300-5963
22. Peters D, Wetzlich J, Thiel F, Seifert Jean-Pierre: Blockchain Applications for Legal Metrology, IEEE International Instrumentation & Measurement Technology Conference (I2MTC), May 14-17, 2018, Houston, Texas
23. European Union Blockchain Observatory and forum, Blockchain and the GDPR, https://www.eublockchainforum.eu/sites/default/files/reports/20181016_report_gdpr.pdf
24. Kosba, A., Miller, A., Shi, E., Wen, Z., & Papamanthou, C. (2016, May). Hawk: The blockchain model of cryptography and privacy-preserving smart contracts. In 2016 IEEE symposium on security and privacy (SP) (pp. 839-858). IEEE.
25. Project "AnGeWaNt", Arbeit an geeichten Waagen für hybride Wiegeleistungen an Nutzfahrzeugen, https://www.arbeitswissenschaft.net/forschung-projekte/angewant/