SN Computer Science (2022) 3:224
https://doi.org/10.1007/s42979-022-01099-9

ORIGINAL RESEARCH

Support for Enhanced GDPR Accountability with the Common Semantic Model for ROPA (CSM-ROPA)

Paul Ryan[1,2] · **Rob Brennan**[1]

Received: 14 September 2021 / Accepted: 19 March 2022 / Published online: 15 April 2022

Abstract

The creation and maintenance of Registers of Processing Activities (ROPA) are essential to meeting the General Data Protection Regulation (GDPR) and thus to demonstrate compliance based on the GDPR concept of accountability. To establish its effectiveness in meeting this obligation, we evaluate an ROPA semantic model, the Common Semantic Model–ROPA (CSM–ROPA). Semantic models and tools represent one solution to the compliance challenges faced by organisations: the heterogeneity of relevant data sources, and the lack of tool interoperability and agreed common standards. By surveying current practice and the literature we identify the requirements for GDPR accountability tools: digital exchange of data, automated accountability verification and privacy-aware data governance. A case study was conducted to analyse the expressivity and effectiveness of CSM–ROPA when used as an interoperable, machine-readable mediation layer to express the concepts in a comprehensive regulator-provided accountability framework used for GDPR compliance. We demonstrate that CSM–ROPA can express 98% of ROPA accountability terms and fully express nine of the ten European regulators' ROPA templates. We identify three terms for addition to CSM–ROPA, and we identify areas where CSM–ROPA relies on partial matches that indicate model limitations. These improvements to CSM–ROPA will provide comprehensive coverage of the regulator-supplied model. We show that tools based on CSM–ROPA can fully meet the requirements of compliance best practice when compared with either manual accountability approaches or a leading privacy software solution.

Keywords Register of Processing Activities · Data Protection Officer · RegTech · Semantic Web · Accountability

Introduction

The GDPR requires organisations to create and maintain a comprehensive record of their personal data processing activities known as a Register of Processing Activities (ROPA).[1] Aside from being a legal obligation on organisations, an ROPA is an internal control tool and is a crucial document to demonstrate that an organisation is meeting the accountability principle of the GDPR [1]. A comprehensive ROPA containing all the processing details in one place will guarantee organisational compliance or identify the organisation's actions to reach this goal [1].

As the scale and complexity of personal data processing carried out by organisations increases [2], and the risks that come with non-compliance with the GDPR, the need for organisations to have a comprehensive and up to date record of their personal processing activities becomes critical [2]. The ROPA practices of organisations vary greatly, with many utilising manual templates to maintain their ROPAs, while others utilise proprietary privacy software solutions [3]. These approaches to ROPA maintenance create significant challenges for the organisation due to the heterogeneity of data sources [4] and a lack of system interoperability with stakeholders such as regulators and processors resulting in compliance challenges for organisations to meet their ROPA obligations [5].

This article is part of the topical collection "Enterprise Information Systems" guest edited by Michal Smialek, Slimane Hammoudi, Alexander Brodsky and Joaquim Filipe.

✉ Paul Ryan
paul.ryan76@mail.dcu.ie

Rob Brennan
rob.brennan@dcu.ie

[1] ADAPT Centre, School of Computing, Dublin City University, Glasnevin, Dublin 9, Ireland

[2] Uniphar PLC, Dublin 24, Ireland

[1] GDPR Article 30.

To date, there has been very little research completed in the area of ROPA. Huth identifies that organisations struggle to conduct the data collection necessary for ROPA [6]. He proposes an Enterprise Architecture approach to generating ROPA [6]. The ONTOROPA project [7], which is in its very early stages, proposes building an ontology and a knowledge graph to generate ROPA and proposes using blockchain to certify the ROPA.

Advances in RegTech provide a source for identifying the best practices for demonstrating regulatory compliance [8]. Previous work identifies a standardised, machine-readable ROPA based on these RegTech best practices as a mechanism to overcome these heterogeneity and interoperability challenges [9]. This will enable the organisation to stay informed of risks, enable regular compliance checks, and support accountability, regardless of the form of the data and the tools generating it [4]. Together the requirements for an accountability system based on machine-readable ROPAs were identified as (i) records the information necessary for the completion of an ROPA and support accountability; (ii) supports the digital exchange of data between parties (and systems) such as processors and regulators; (iii) supports automated accountability compliance verification; and (iv) integrates with privacy-aware data governance processes and tools [10].

This research brings together learnings from RegTech [11] to identify the requirements for automated GDPR accountability systems [10]. These learnings are utilised to develop the common semantic model of ROPA [9]. We gain valuable insights into the application of RegTech best practices in a GDPR context as we move from theory to practice. We present a use case where we deploy CSM–ROPA to support automated compliance with a regulator accountability framework. Our research question asks, what is the effectiveness of CSM–ROPA in assisting organisations to meet automated compliance best practice requirements and support their compliance with the accountability principle of the GDPR?

This paper is an extended version of the paper "Demonstrating GDPR Accountability with CSM–ROPA: Extensions to the Data Privacy Vocabulary" presented at ICEIS2021 [12]. The extensions and revisions of this paper are as follows:

- We detail the reasons why organisations require a machine-readable ROPA
- We derive the requirements for automated GDPR accountability from best practices
- We identify the system requirements for automated GDPR accountability based on a machine-readable ROPA
- We build on our previous work to demonstrate the extent of expressivity of CSM–ROPA to meet the expectations of a regulator supplied accountability framework.
- We evaluate how CSM–ROPA compares to manual approaches and the leading privacy software provider, "One Trust", in meeting the key requirements for GDPR accountability tools.

Section 2 will discuss what accountability means under the GDPR and how the tools available to organisations to demonstrate accountability are largely inadequate. Section 3 presents a review of the ROPA handling practices of organisations. We show that they face challenges with maintaining their ROPA documents. We identify that many ROPAs are generalised and vague, contain insufficient detail, and lack consistency. Many ROPAs are in a form that prevents interoperability with other stakeholders. We show that organisations struggle to harvest and maintain the data required for GDPR accountability despite significant financial investment by organisations.

We provide an overview of CSM–ROPA and a case study-based evaluation of CSM–ROPA's ability to express a regulator provided accountability framework to support the demonstration of accountability. We also evaluate the ability of CSM–ROPA to meet the requirements of a machine-readable ROPA compared to a manual approach and a leading proprietary privacy software solution. The remainder of this paper discusses the requirements for a machine-readable ROPA to support automated accountability; we establish best practices for regulatory compliance from RegTech and provide a derived system requirement for automated GDPR accountability.

Defining Accountability Under the GDPR

Accountability is an expression of the conduct and behaviours of an organisation. They must show that they act in an open, fair and equitable way [13]. The evolution of accountability within data protection law stems from the OECD privacy guidelines of 1980, which introduced accountability as a basic principle [14, 15]. These guidelines require that organisations comply with the measures that affect the principle of accountability [15]. The evolution of data protection accountability continued over the next 30 years in areas such as trust marks, where organisations obtain verification that they adhere to good privacy practices [15] and the development of rules for international data transfers where organisations completed self-certification exercises to show that they acted in an accountable manner. Over time a lack of inconsistent standards and accountability verification by regulated bodies brought about a renewed impetus for verifiable accountability [15]. In 2010, the EU Article 29 Working

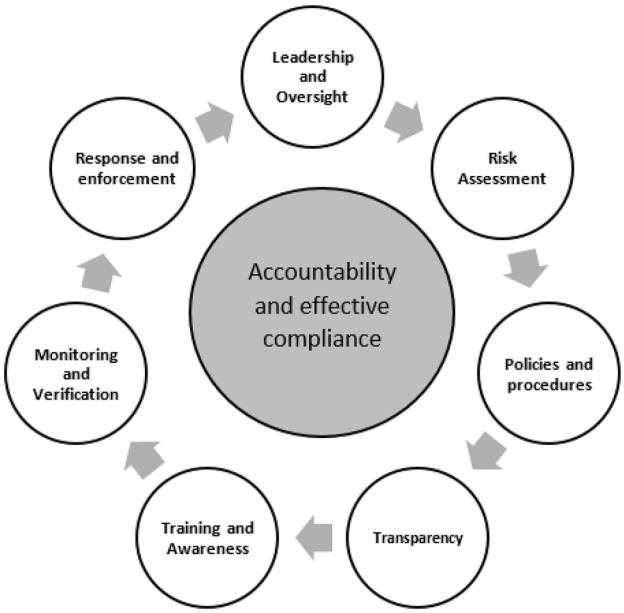

Fig. 1 CIPL accountability wheel–universal elements of accountability [20]

Party [16] brought data protection accountability to a new level of legal certainty when they required that data controllers must put in place appropriate and effective measures to ensure that the obligations and principles set out in the Data Protection Directive (1995) [17] are complied with. They must demonstrate this accountability to data protection regulators upon request [16].

The introduction of the GDPR in 2018 set accountability as a cornerstone of its principles and clearly stated that data protection was no longer considered an optional extra for organisations [18]. The burden of ensuring that personal data processing is legal now falls primarily on the organisation [18]. The organisation must demonstrate this compliance to external stakeholders, such as individual data subjects, business partners, and civil society bodies representing individuals and Data Protection Authorities. The GDPR gives such emphasis to the term "demonstrate" compliance that it appears 33 times in the GDPR [19]. The challenge for organisations is that they must put be able to show that they have appropriate and effective data protection measures in place to demonstrate that they are meeting their obligations as set in the GDPR.[2]

An accountable organisation needs to ensure that it can evidence its compliance across the 99 GDPR articles, which can be a substantial undertaking. The Centre for Information Policy Leadership (CIPL) "Accountability Wheel" [20] in Fig. 1 identifies the essential elements of organisational accountability.

Many organisations have utilised this framework for compliance demonstration using maturity models, self-assessment tools and accountability trackers.

Maturity models have been utilised as a tool for compliance monitoring for many years [8]. These models are used to understand an organisation's privacy compliance standing. A question set consisting of "generally accepted privacy principles" is gauged along an axis of maturity from ad hoc to optimised. There have been some GDPR specific maturity models developed, such as the International Association of Privacy Professionals (IAPP) Maturity Framework [21] developed with a series of checklists built through a collaboration with a team of experienced privacy and security professionals, lawyers and regulators [21]. A review of privacy maturity models as an accountability tool finds a need to elaborate a GDPR-specific model that addresses the relevant requirements to achieve compliance [22]. The review suggests that a new privacy maturity model would support decision-makers in deciding which measures to take on the road to privacy compliance. The elaboration of this model would pave the way for further research and could provide a specific tool for organisations to measure their privacy management activities. The key failings of maturity models for GDPR compliance verification are as follows [8]:

- they are highly dependent on domain experts and are labour intensive
- the methods can be prone to human subjectivity, errors and bias
- models are infrequently updated
- the measures often require academic validation
- they are unsuitable as part of an automated process and improvement toolchain

While maturity models indicate an organisation's GDPR compliance position, their numerous limitations prevent these tools from developing further without automation.

To assist the organisation in meeting its GDPR accountability obligations, several data protection regulators have developed checklists,[3] guidance documents, and self-assessment toolkits.[4] These assessment tools are fundamentally high-level resources to help the organisation gain a broad, high-level assessment of their GDPR compliance [8], which rely on the qualitative input of users in checklists. To add to organisations' challenges, many of these templates differ across jurisdictions [8]. However, they do offer a key benefit

[2] GDPR Art. 5.

[3] Self-Assessment Checklist | Data Protection Commissioner.

[4] Record of processing activities—Data Protection Ombudsman's Office (tietosuoja.fi).

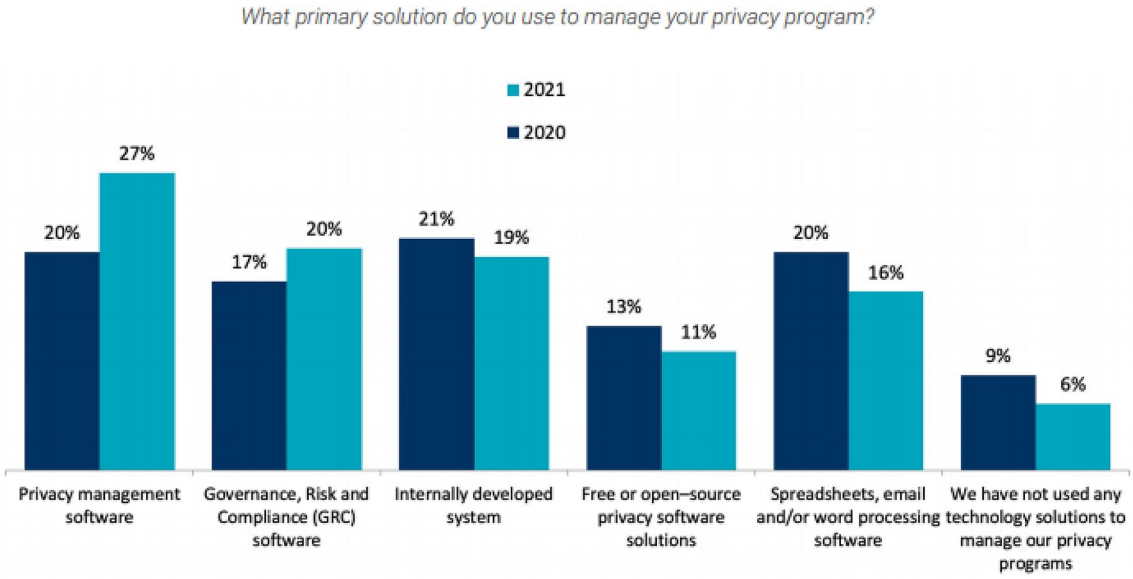

Fig. 2 Primary solution used to manage privacy program [3]

in that they have been developed by regulators. Some regulators have made progressive initiatives to assist organisations in demonstrating their compliance, such as the United Kingdom data protection regulator, the Information Commissioners Officer (ICO). In 2020, the ICO published their accountability framework,[5]which they describe as a resource for organisations, large or small, to assess the effectiveness of the accountability measures that they have in place and understand where they need to improve [23]. The ICO accountability framework contains the same essential elements as the CIPL accountability wheel [24], but expresses these elements over ten specific GDPR accountability categories. This framework was developed with privacy professionals, legal experts and the regulator. We discuss the framework in more detail as part of our case study in Sect. 7.

Organisations are challenged with demonstrating GDPR compliance [3, 3]. The heterogeneous nature of GDPR accountability data [4], the extent of the data processing chain (which may contain numerous stakeholders), and the rate of business process change require that the Data Protection Officer (DPO) has visibility of the most up to date information concerning the personal data processing activities of the organisation. The challenge organisations face is gaining and maintaining this visibility of their compliance level and their processors [4]. The accountability principle has placed a legal obligation on organisations to demonstrate compliance. To date, EU regulators have issued €1.5 billion in fines [25]. Hence, the challenge for organisations is to identify their GDPR compliance GDPR level and close any gaps. In the next section, we will evaluate how organisations approach the critical area of ROPA compliance to understand the challenges they face in supporting accountability.

A Survey of Organisational Approaches to ROPA Compliance

When we consider the importance of ROPA as a control tool for GDPR compliance [1], we analyse how organisations are approaching the generation and ongoing maintenance of their ROPAs. A recent survey reviewed the ROPA practices of 30 public organisations and found that only 7 (23%) of the organisations ROPAs contained sufficient detail for the purpose [5]. Among the shortcoming identified in this survey are:

- Many of the ROPAs appear to be generalised and vague
- ROPA not being kept up to date
- Organisation defaulting ownership of ROPA to the DPO
- The ROPA presents an inventory of records and does not detail the processing activities
- ROPA lacks sufficient details of technical and organisational security measures in place
- Declared retention periods inaccurate or incomplete
- Inconsistent approaches to the maintenance of ROPA

Organisations are very much struggling with their ROPA compliance [5]. They fail to consistently and comprehensively document their processing activities on their ROPA. Many organisations are devolving responsibility for ROPA to the DPO when the organisation itself is responsible for

[5] https://ico.org.uk/for-organisations/accountability-framework/

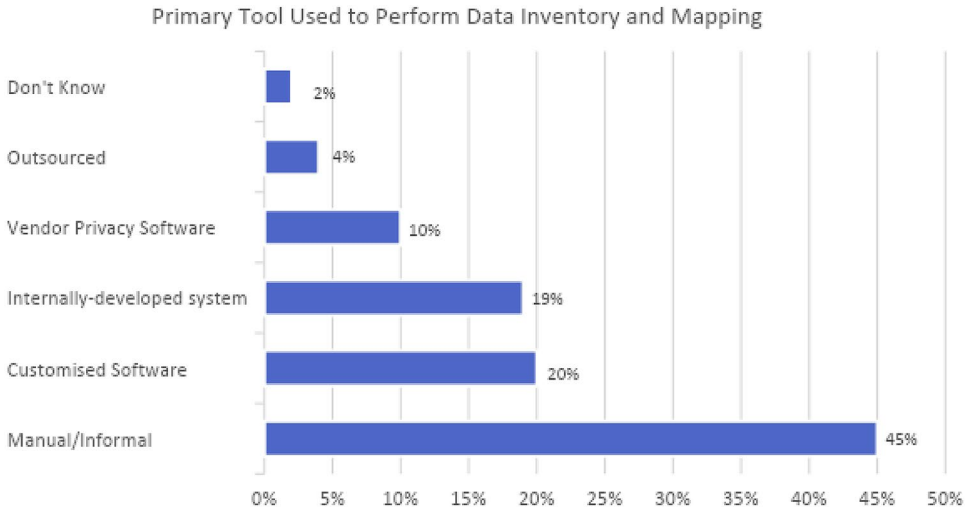

Fig. 3 Primary tool used by organisations for data inventory and mapping [3]

demonstrating compliance and not the DPO. They are exposing themselves to significant risks in this area.

We see a very fragmented approach to how organisations approach GDPR compliance. The approach taken by organisations is very varied, as seen in Fig. 2 [3]. It shows that 22% of organisations create and maintain ROPAs through informal tools like spreadsheets or have no tools [3]. The United Kingdom Data Protection Regulator (ICO) indicates that organisations commence the ROPA process by conducting an information audit or data-mapping exercise. This will clarify the organisation's data and where they hold it. The process requires a cross-organisation approach to ensure that the organisation is fully engaged in the process. This approach ensures that the organisation does not miss anything when mapping the data processed by the organisation. Several data protection supervisory authorities have provided ROPA templates to assist organisations to complete their ROPA. These documents are spreadsheet-based templates, and they vary significantly between regulators [9]. These solutions are primarily spreadsheet-based and rely on the qualitative input of users, and they lack interoperability with other solutions. In 2019, the International Association of Privacy Professionals (IAPP) examined ROPA compliance in more detail [3]. The IAPP found that almost half (45%) of organisations completed their data mapping and inventory operations using manual/informal tools, such as spreadsheets, email, and in-person communication (Fig. 3). A further 10% of organisations utilised vendor-supplied software off the shelf [3].

There has been considerable investment by organisations in privacy software. Many organisations invest in technology solutions such as privacy software, thus reducing the number of organisations reliant on spreadsheets or wholly manual solutions. The worldwide data privacy market grew by 60.29% in 2019 [26], with many vendors entering this market (see Fig. 4). While vendors offer a variety of privacy software solutions, there is no single privacy software that will automatically make an organisation GDPR compliant [27]. The number of new vendors of privacy software solutions has proliferated over the last 5 years (see Fig. 5) [28]. According to IAPP, there are one hundred and sixty-nine vendors supplying data mapping, data inventory and ROPA software [28] as of 2020. The key challenges with vendor-supplied ROPA software [10] are as follows:

- They are standalone and lack interoperability
- They focus on largely manual or semi-automated approaches that are labour intensive and rely on domain experts
- The development of these systems occurs without the input of the regulator.
- They lack standards-based approaches to compliance

Organisations face significant difficulties when implementing GDPR best practices due to a lack of common ground between the legal and data management domains [29]. The data protection context has been led mainly by legal professionals who have limited insight into the

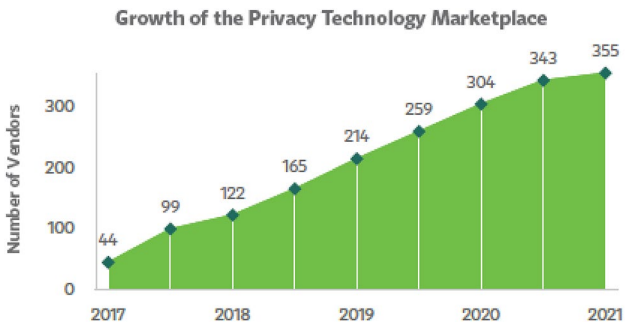

Fig. 4 Growth of privacy technology marketplace [28]

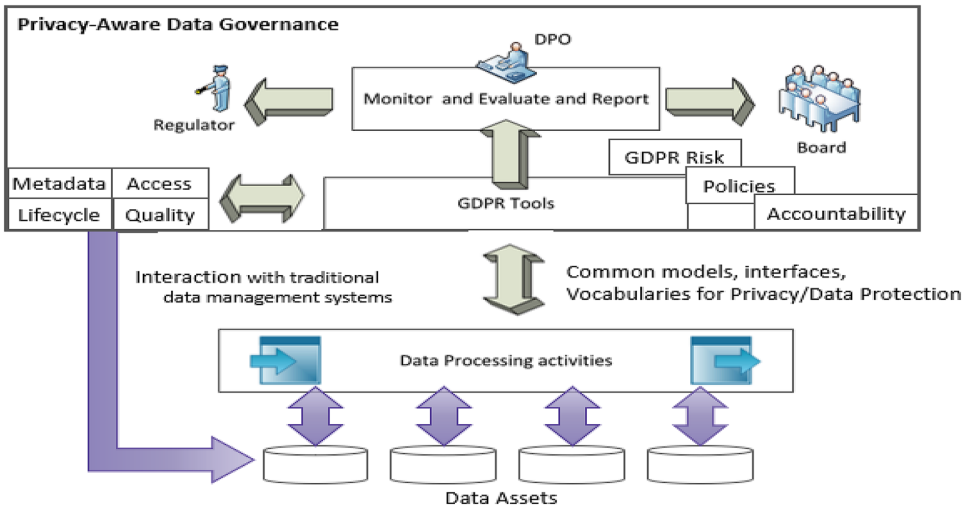

Fig. 5 Privacy-aware data governance to support GDPR RegTech [12]

opportunities native digital methods provide. This approach has resulted in ad hoc, manual or semi-automated organisational processes and tools for data protection that are not fit for purpose and limit organisational change [10]. For example, only 3% of data subject access requests are automated, and 57% are entirely manual [3]. For some privacy tech offerings, it is unclear whether vendor-developed privacy tech is sufficient to satisfy the regulatory compliance or business needs of would-be purchasers [30]. Organisations' critical challenge is to evolve from the existing ROPA compliance solutions where ROPA are created and maintained through informal tools and spreadsheets [3].

Requirements for a Machine-Readable ROPA

This section shows why organisations need to implement a machine-readable ROPA. The GDPR requires the DPO to access the most up to date and comprehensive data processing information. The DPO must monitor, advise, and inform the organisation of any non-compliance with the GDPR. The challenge for the DPO is to gain this visibility of the GDPR accountability data. The heterogeneity of data sources, the lack of interoperability with data processing partners and the complex scale of data processing provides the DPO with significant challenges in gaining and maintaining this visibility.

A cross-sectoral study conducted in 2019 across ten countries and among more than 1100 executives reported that only 28% of the responding organisations were compliant with the GDPR at that time [31]. This low level of GDPR compliance is a significant risk for organisations, so why are they failing to be compliant? Jakobi et al. describe the three approaches organisations are taking for dealing with the GDPR in day-to-day business [32]. These strategies stretch from burying the head in the sand to compliance to the minimum level against a first-time fine to the few organisations that see compliance as a quality feature for their business customers or end-users seeking to generate competitive advantage from GDPR compliance.

Many data protection authorities agree that to have a good overview of an organisation's processing activities, the ROPA is a vital element [33]. Aside from being a legal obligation on organisations to maintain an up to date ROPA, the record is an internal control tool and is a way to demonstrate an organisation's compliance with GDPR.[6]It is a comprehensive record of an organisation's personal data processing activities. It is integral to meeting the principle of accountability as set out in Article 30 of the GDPR. It provides an overview of the ongoing data processing operations and helps organisations decide which appropriate technical and organisational measures to manage risk within their personal data processing activities. In addition, the ROPA supports the drafting and updating of privacy notices, as the ROPA contains much of the information required for these notices. Finally, the information included in the ROPA assists the organisation in determining if processing activities meet the threshold of high risk and thus need to be part of a Data Protection Impact Assessment (DPIA) [34].

As the scale and complexity of data processing carried out by organisations becomes more complex, and the consequences of organisational non-compliance with the GDPR are laid bare, the need for the DPO to have a comprehensive overview of the data processing activities is critical. A machine-readable ROPA will significantly benefit the DPO to enable regular compliance checks. The ROPA provides the DPO with a direct view of the front line [2] and helps keep the DPO informed of risks irrespective of the source or form of the data. An accountable organisation must maintain an ROPA that reflects the reality of the organisations

[6] https://www.cnil.fr/en/record-processing-activities

processing operations [16]. This means that the ROPA must reflect the actuality of the processing activities and, most important, must be kept up to date [19]. A machine-readable ROPA will provide the DPO with the toolset to continually monitor the data protection compliance of the organisation. The machine-readable ROPA becomes particularly beneficial when regulatory changes occur, such as new interpretations of existing laws, new adequacy decisions on data transfers or new laws, as the DPO has visibility of the processing activities to conduct an immediate analysis.

The machine-readable ROPA benefits organisations when considering new or modified personal data processing activities. While there are some accountability measures that you must take when changing and adding new processes, such as completing a data protection impact assessment for high-risk processing, the ROPA must be checked to evaluate if it needs updating. The machine-readable ROPA will help to inform the DPO if the new or modified process that is created is compliant. This check is integral to the change management process [16]. The manual nature of maintaining ROPA can make this manual task that can be easily missed [2].

Compliance monitoring can be extended beyond the organisation's boundary when a machine-readable ROPA model is deployed. This use of a consensus-based vernacular model can facilitate the digital exchange of compliance information between stakeholders, such as processors and controllers, thus building trust and confidence in the data processing chain. Similarly, the machine-readable ROPA could be deployed to support machine to machine accountability compliance verification between the organisation and regulators. An organisation may also need to demonstrate compliance as part of a code of conduct, a certification body, or as part of a standardised certification accountability framework (GDPR Art 42). The role of such external certifications, seals and codes of conduct has the added benefit to support accountability when accompanied by some form of external validation, which ensures both demonstration and verification [35]. A machine-readable ROPA would facilitate the sharing of accountability data with such certification bodies, thus improving the visibility of the accountability practices of the organisation.

System Requirements for Automated GDPR Accountability Based on a Machine-Readable ROPA

This section reviews the literature identifying best practices for demonstrating regulatory compliance. Our research yielded very little direct research of GDPR compliance; however, a body of relevant research in RegTech was identified. The catalyst for the emergence of the RegTech approach to regulatory compliance was the Global Financial Crisis of 2007. The introduction of many financial regulations, significant regulatory fines and increasing operational costs created great challenges to organisations. The financial industry's response was RegTech to overcome the increasing compliance challenges they were faced with [11]. We identified the four key features of RegTech systems to enable organisations to demonstrate compliance with regulations successfully. These features enable a well-defined data governance capability, the application of ICT advances to regulatory compliance, the agreement on agreed semantics/common standards to facilitate and enable the interoperability of systems, and the proactive role of regulators as facilitators for the automation of regulation [11]. These features will be discussed in detail in the following sub-section.

Enabling a Well-Defined Data Governance Capability

Despite many organisations embracing the productivity and agility gains of digitalisation, they continue to struggle with the basic principles of data governance [11]. Organisations require a dedicated data governance capability to build common ground between the legal and data management domains [29], facilitate the digital transformation of organisations [8, 36], and enable effective control and monitoring of data processing assets for compliance purposes [36]. Organisations need to define data principles clearly and treat data as assets [37]. The agreed uses that data is put to must be clearly defined, and the organisation must ensure that the use of data positively relates to the regulatory environment. Organisations need to define the agreed behaviours and policies for data quality, who will access the data, how data is interpreted, and how long the data will be retained. Applying a structured data governance approach to organisational data, coupled with agreed semantics, can enable the smooth and efficient flow of data between parties, thus bringing efficiencies to the organisation [12] (see Fig. 5). The challenge organisations face regarding personal data is locating, classifying, and cataloguing this accountability data. Once the organisation can gather these data, the organisation can create appropriate metadata to enable management of the personal data and then deploy a policy monitoring and enforcement infrastructure leveraging that metadata to assure lawful data processing generates appropriate compliance records [38].

Applying ICT Advances to GDPR Accountability

The use of technology to streamline regulatory compliance in the financial services sector continues to be a fast-moving and fast-growing sector. A key driver at the forefront of RegTech success has been adapting new technologies [39]. The Fintech revolution [40] brought about the implementation of Big Data storage, collection, and analytics techniques such as

machine learning, natural language processing (NLP), Artificial Intelligence (AI), cloud technology, DevOps (continuous development), distributed ledgers technology like blockchain, semantic integration tools and many other technologies into the financial industry. The growing cost of compliance and the need for agile solutions brought about the speedy and effective implementation of such new technologies. The transformative nature enjoyed by RegTech offers opportunities in the GDPR context by applying such technologies to facilitate interoperability between stakeholders [41]. A RegTech approach to GDPR compliance will require organisations to implement such technologies in the GDPR ecosystem to facilitate efficient and effective compliance [8].

Agreement on Common Standards and Agreed Semantics for Personal Data Processing

The third requirement for GDPR RegTech is making personal data interoperable between systems. The digitalisation of financial data in RegTech has enabled the application of technology to this data; this may not be so easy to achieve in a GDPR environment. Cataloguing and discovering personal data are becoming a big topic for business analytics. Many companies have invested heavily in discovery tools to harvest data for data subject access requests and ROPAs [28]. This process provides an excellent opportunity to harvest the data for more automation of accountability. The semantic modelling of personal data processing activities would greatly benefit an organisation and provide for machine-readable and interoperable representations of information, thus allowing queries to be run and verified based on open standards, such as Resource Description Framework (RDF), SPARQL protocol, W3C Web Ontology Language (OWL) and Shapes Constraint Language (SHACL) [42]. Combining legal knowledge bases with these models becomes beneficial to compliance evaluation and monitoring, which can help harmonise and facilitate a joint approach between legal departments and other stakeholders to identify workable and compliant solutions around data protection regulations [29]. The Semantic Interoperability Community (SEMIC) has progressed in this area by developing Core Vocabularies that provide a simplified, reusable and extensible data model for capturing fundamental characteristics of an entity in a non-domain specific context [39] to foster interoperability. This work continues to be built on by developing the W3C Data Privacy Vocabulary (DPV) and the PROV-O Ontology [42].

Data Protection Supervisory Authorities as an Enabler

The fourth requirement for GDPR RegTech requires proactive regulators to work with organisations to automate regulation and make compliance easier to achieve. To date, GDPR regulators have lacked such proactive in comparison with financial regulators, who have actively facilitated the automation of digital compliance. GDPR regulators have been quite slow to take a similar role in automated GDPR compliance compared to financial regulators. This lack of leadership has resulted in organisations facing the pitfalls of a fragmented "Tower of Babel" approach [9] due to a lack of a common agreed semantic vocabulary. Our analysis of RegTech [8, 9] has shown that compliance monitoring and reporting to improve compliance monitoring is achievable using technology when combined with flexible, agile, cost-effective, extensible, and informative tools. When regulators enable and facilitate digital compliance, actively promote and enable digital regulatory compliance standards, and act as enablers for the automation of regulation, they actively create an environment for digital compliance [11, 43]. For GDPR RegTech to succeed, GDPR regulators will need to move towards a symbiotic relationship with technology innovators and organisations that process personal data to develop open-source compliance tools, digital regulations, tech sprints, and sandboxes [40]. These collaborative initiatives help build an essential environment to foster technology application to meet regulatory obligations and advance RegTech [11]. The role of the supervisory authority is that of a critical enabler and a facilitator for GDPR RegTech. Regulators need to close the gap between the intention of regulatory requirements and the subsequent interpretation and implementation within firms. Regulators need to utilise technology that simplifies and assists firms in managing and exploiting their existing data, supporting better decision-making, and finding those who are not playing by the rules easier. These collaborative initiatives would significantly accelerate the successes of GDPR RegTech solutions.

Final Derived Requirements for Automated GDPR Accountability

Our literature review has identified the best practices for demonstrating regulatory compliance and GDPR accountability. We take the four best practices from RegTech and build on these to create a list of the following requirements:

R1: Records the information necessary for the completion of an ROPA and demonstrate accountability

- Supports the heterogeneity of data sources required
- Spans application-centric data silos
- Spans organisational and functional units
- Interlinking capability—any relevant models or data can be linked

R2: Supports the digital exchange of data between parties (and systems) such as processors and regulators

- Standards-based approach, defining:
  - Data formats—data are available in a common agreed semantic standard, e.g., RDF
  - Protocols/interfaces for transfer and access
  - Processes and compliance points
  - Common definitions of terms

R3: Automated accountability compliance verification

- Semantic models/support for inference
- Standards as per R2

R4: Privacy-Aware Data Governance

- Integration with organisational data governance processes, roles and data management systems, so these and their metadata can be reused for GDPR compliance and governance
- Supports risk-based data governance
- Specifies machine-readable data protection and data processing policies
- DPO-centric tools to monitor, evaluate and report on GDPR compliance
- Reporting/digital exchange with internal and external GDPR stakeholders
- Methods and tools to manage the accountability metadata lifecycle, e.g., data quality assurance of accountability data

CSM–ROPA Overview

In Sect. 3, we have shown how organisations are struggling to maintain ROPAs, which is a crucial element to demonstrate their GDPR compliance. We have shown that whilst many organisations are moving towards technology for compliance (Fig. 4), many are still choosing to complete their ROPAs using manual processes (Fig. 3) and are failing to take cognisance of best practices. In Sect. 4, we identified established best practices for demonstrating regulatory compliance based upon the experiences gained from RegTech. The development of CSM–ROPA is motivated to harness these best practices and semantically express regulator supplied ROPAs. Section 5 specified the system requirements for automated accountability based on a machine-readable ROPA to assist the Data Protection Officer with accountability compliance.

CSM–ROPA is a semantic model developed based on the GDPR requirements identified in six English language ROPA templates that EU Data Protection Regulators provided. CSM–ROPA is a profile of the Data Privacy Vocabulary (DPV)[7] and utilises the base specifications, semantic interpretations and concepts to model ROPA.[8]The DPV is a domain-independent vocabulary that can be extended or specialised for specific domains or use-cases. This vocabulary is utilised in many use cases, and many projects have declared their interest in its adoption [9, 44, 45]. The DPV organises its concepts in a lightweight taxonomic structure [46] using RDFS, the W3C resource description framework (RDF) schema language.

The methodology used for ontology engineering and development lies in the reuse and subsequent reengineering of knowledge resources, collaborative and argumentative ontology development, and building ontology networks. The creation of the DPV ontology follows guidelines and methodologies deemed best practices by the Semantic Web community [47]. It follows the NeOn methodology [48] and UPON Lite methodology [49] for vocabulary development. The development of CSM–ROPA uses the Action Design Research (ADR) methodology [50]. This research method generates prescriptive design knowledge by building and evaluating the CSM–ROPA artefact in an organisational setting. The ADR design approach deals with the disparate challenges of addressing an organisational problem situation and constructing and evaluating an IT artefact that addresses the problem situation. This methodology focuses on the building, intervention, and evaluation of an artefact that reflects not only the theoretical precursors and intent of the researchers but also the influence of users and ongoing use in the context. As CSM–ROPA is developed, numerous stakeholders and users will contribute to an iterative approach where the artefact is gradually built out.

The Data Privacy Vocabulary was first released in July 2019. The vocabulary aims to provide a basic vocabulary of terms related to the data protection and privacy domain framed by the GDPR. The vocabulary relies on RDF, RDFS, SKOS and OWL. The DPV consists of ten modules such as personal data category, purpose and risk that provide a taxonomy of terms related to personal data processing.

Section 2 detailed the organisation's obligations to demonstrate compliance to internal stakeholders such as the organisation's board and external stakeholders such as individuals, business partners, shareholders, and Data Protection Authorities. It is envisaged that CSM–ROPA is deployed as a mediation layer (see Fig. 6) between the organisations business processing layer and the reporting and monitoring layers to enable organisations to meet these obligations. CSM–ROPA has evolved to support automated and semi-automated accountability compliance verification [4, 7]. CSM–ROPA has evolved from the application of RegTech

[7] https://dpvcg.github.io/dpv/

[8] https://www.w3.org/2017/dxwg/wiki/ProfileDescriptors

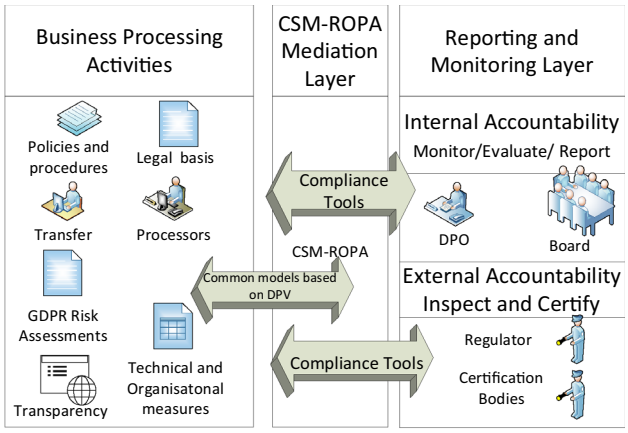

Fig. 6 CSM–ROPA as a mediation layer [12]

best practice and is designed to develop platforms and tools that allow for the smooth interoperation of systems [7]. Using CSM–ROPA to create and maintain the organisation's ROPA will enable automated ROPA accountability compliance verification and interoperability with regulators and certification bodies alike [7].

Case Study

This section examines a potential deployment of the CSM–ROPA data model. We evaluate the extent to which an organisation can utilise the CSM–ROPA as a mediation layer to demonstrate ROPA compliance and as a basis for developing compliance tools. For this analysis, we select the ROPA section of the ICO accountability framework, where the regulator has determined the expectations that must be met as the basis for evaluation. We map all terms in the ROPA section of the framework to establish how CSM–ROPA can express the individual terms and each of the ten expectations of the ICO framework.

The ICO accountability Framework tracker is spreadsheet format. It is a manually maintained static, standalone entity. It does not facilitate interoperability with any system, thus significantly increasing the likelihood of not being managed or maintained.

In 2020, the ICO published their accountability framework,[9] which they describe as a framework for organisations, large or small, to assess the effectiveness of the accountability measures they have in place and understand where they need to improve [23]. The ICO accountability framework contains the same essential elements in the CIPL accountability wheel [20] but expresses these elements over ten specific GDPR accountability categories. Each category contains several expectations (of how an organisation can demonstrate accountability), and each of the 77 expectations contains many detailed questions (see Table 1). The framework provides the necessary detailed granularity that enables an organisation to evaluate their level of compliance relative to each statement using a four-level scale which ranges from not meeting/ partially/ fully meeting this expectation or as "not applicable".

Table 1 ICO accountability framework categories, expectations and questions

ICO category	No. of expectations	No. of questions
Leadership and Oversight	6	33
Policies and procedures	4	17
Training and awareness	5	17
Individuals' rights	11	42
Transparency	7	31
Records of processing and the lawful basis	10	33
Contracts and data sharing	9	31
Risks and Data Protection Impact Assessments	5	29
Records management and security	12	63
Breach response and monitoring	8	38
Totals	77	334

https://ico.org.uk/for-organisations/accountability-framework/

The ICO accountability framework has several uses for organisations, such as recording, tracking, and reporting compliance progress. It can check the organisation's existing practices against the ICO's expectations to identify where they could improve existing practices and clearly understand how to demonstrate compliance and increase senior management engagement and privacy awareness across an organisation. GDPR accountability should extend across the entire operating system, wherever risks are managed, including shared risks that cross organisational boundaries [23]. At the same time, accountability should be escalated up and down a reporting hierarchy from operational level to system regulator.

Methodology

We evaluate to what extent CSM–ROPA can semantically express the terms found in the ROPA category of the ICO accountability framework.[10] Our methodology for this case study consists of the following steps:

[9] https://ico.org.uk/for-organisations/accountability-framework/

[10] Paul-Ryan76/ICO2CSM-ROPA: Mapping of ICO Accountability Tracker Sect. 6 to CSM-ROPA (github.com).

Table 2 Sample of mapping outcomes

Unique term in ICO Accountability Framework	Matching concept(s) in CSM–ROPA	Mapping/proposed action
The purposes of the processing	dpv: Purpose	*Exact match*—the term can be fully expressed using the existing vocabulary of the DPV
Contact details	None	*Other vocabularies*—the term can be fully expressed using an alternative vocabulary like the vCard Ontology[a]
Preference-management tools	dpv:TechnicalMeasure; dpv:Consent; dpv:hasWithdrawlMethod	*Complex match*—the term can be fully expressed using multiple terms from the existing vocabulary of the DPV
A 'balancing test.'	dpv:LegalBasis; dpv:Context; dpb:Risk	*Partial match*—the term cannot be fully expressed using multiple terms from the existing vocabulary of the DPV; only a partial expression is achieved
The transfer mechanism safeguards	None	*New Term*—the term has been submitted to the DPVCG[b] and is under consideration for addition to the DPV vocabulary

[a]https://www.w3.org/TR/vcard-rdf/

[b]Data Privacy Vocabularies and Controls Community Group https://www.w3.org/community/dpvcg/

- Select the ROPA category within the accountability tracker for analysis
- Identify the unique terms (concepts and relations) stated in each accountability expectation (see Table 2)
- Compare the unique terms found in the ROPA category to CSM–ROPA terms to evaluate if there is a corresponding exact semantic match of each other or a partial match, or no match [51]
- For terms where we find no match with CSM–ROPA, we evaluate if the term exists in another well-known linked data vocabulary and, if so, use the additional vocabulary to model the unique term and add it to the CSM–ROPA profile definition.
- For the remaining terms, we make a recommendation for its inclusion in DPV if relevant
- Each of the ten expectations stated in Sect. 6 of the ICO Accountability Framework establishes how effective CSM–ROPA is in expressing each expectation. Compare the terms within each expectation to CSM–ROPA and measure the match % for each expectation in terms of a corresponding exact semantic match; mapping can be completed using other vocabularies, complex mapping, partial mapping or no mapping or under consideration with Data Privacy Vocabularies and Controls Community Group (DPVCG).
- Evaluate how effective CSM–ROPA is at expressing each expectation and identify where CSM–ROPA requires additional terms where mapping is not possible or where CSM–ROPA achieves only partial matches

Analysis

We select the ICO Accountability Framework records of processing and lawful basis category for analysis for this case study. This category contains all relevant expectations for ROPA compliance demonstration as determined by the regulator. We identified 192 terms (concepts or relationships in a knowledge model) used by the ICO in these questions. When we remove duplicate terms, 139 unique terms remain. We evaluated these unique terms to establish if it was possible to semantically express them using existing terms in CSM–ROPA (see Table 3 for examples of outcomes).

The outcome of our mapping (see Table 3) showed that CSM–ROPA could express 55% of the unique terms precisely. Another 43% are expressed using a combination of complex, partial mapping or other vocabularies. CSM–ROPA did not have the expressiveness to model three

Table 3 Summary of mapping results

Outcome of mapping	No. of terms	% of terms (%)
Exact mapping one to one	77	55
Mapped using other vocabularies	12	9
Complex mapping	15	11
Partial mapping	32	23
No mapping, under consideration with DPVCG	3	2

Table 4 Expressiveness of CSM–ROPA to model Sect. 6 of the ICO accountability framework

Expectation no	ICO expectations section	Exact match	Other vocabulary	Complex match	Partial match	DPV under consideration	Grand total
6.1	Data-mapping	5	3	1		5	14
6.2	ROPA—process	5	1	1	5		12
6.3	ROPA article 30 compliance	16	2			1	19
6.4	Good practice for ROPAs:	13					13
6.5	Documenting your lawful basis:	18	2	2	7		29
6.6	Lawful basis transparency:	9	1	2	3		15
6.7	Consent requirements:	17		4	6		27
6.8	Reviewing consent:	8	1	1	2		12
6.9	Risk-based age checks/ guardian consent	18	6	4	3		31
6.10	Legitimate Interest Assessment (LIA)	9	1	2	8		20
	Totals:	118	17	17	34	6	192

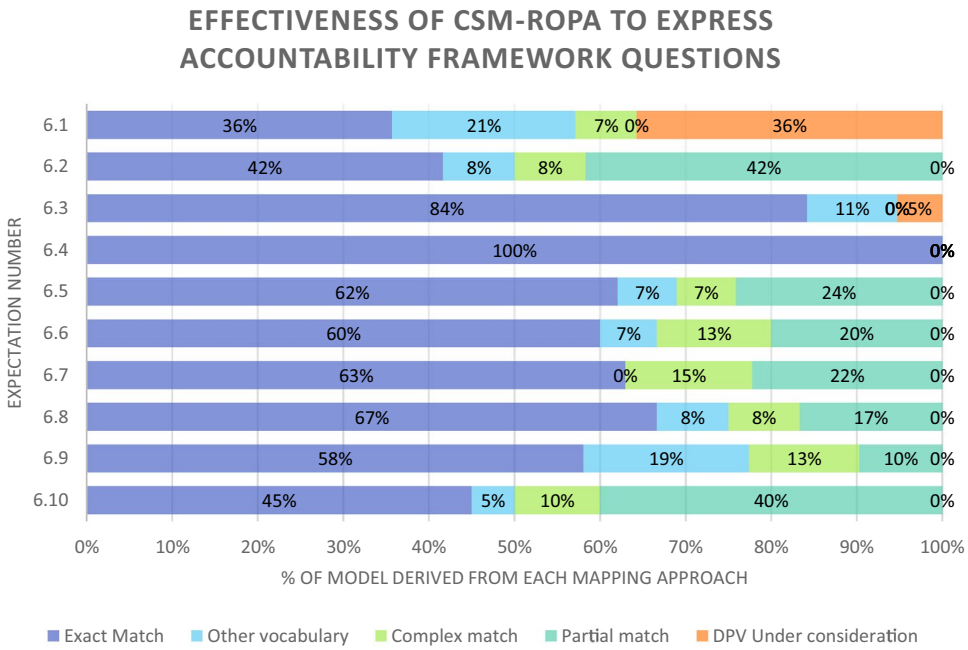

Fig. 7 Effectiveness of CSM–ROPA to express accountability framework questions

terms, equating to 2% of the unique terms. We have identified other vocabularies that could map 12 of these terms: date/time and age-related terms. See Table 3 below for a summary of all mapping results.

Our analysis shows that CSM–ROPA can express 92% of the terms found in the ICO Accountability Tracker. When we supplement CSM-ROPA with additional vocabularies we find that we can express 98% of the Accountability Tracker. For the three terms that cannot be mapped, we have submitted these for inclusion in the DPV and CSM–ROPA to the Data Privacy Vocabularies and Controls Community Group (DPVCG)[11]. These terms are "Appropriate Safeguards for Third Country Transfers", "Data Map", and "Legislation". Adding three identified terms to CSM–ROPA will enable the ICO Accountability Framework ROPA category to complete mapping.

In Table 4, we show the effectiveness of CSM–ROPA to express each of the individual expectations, to establish the extent that CSM–ROPA can express each expectation. When we look at each of the ten ICO accountability expectations individually and in specific terms that ICO uses for each expectation, we find that CSM–ROPA can express each expectation with varying fidelity. We find that for some expectations, CSM–ROPA is very successful in precisely modelling the terms used in the expectation (and storing the required evidence or supporting automated validation

[11] https://www.w3.org/community/dpvcg/

Table 5 Comparison of approaches to operationalising GDPR accountability

System requirements	Manual approaches	One trust privacy	CSM–ROPA
R1: Records the information necessary for the completion of an ROPA and demonstrate accountability	☒	☒	☒
R2: Supports the digital exchange of data between parties (and systems), such as processors and regulators	☐	☐	☒
R3: Automated accountability compliance verification	☐	☐	☒
R4: Privacy-Aware—Data Governance	☐	☒	☒

of the expectation). An example of such full expressivity is 6.3 ROPA article 30 compliance and 6.4 good practice for ROPAs, where CSM–ROPA can express the expectation completely with exact matches and other vocabularies. We identify that several expectations such as 6.2 and 6.10 utilise partial matches for over 40% of their terms, while three other expectations, 6.5, 6.6 and 6.7, are partially matched for 20–24% of terms (see Fig. 7).

Our analysis has identified the following key findings:

- The ability of CSM–ROPA to express 98% of terms and nine of the ten expectations of the ROPA section of ICO the accountability framework.
- Expectation 6.2 "ROPA Process" contains three terms requiring the addition of the DPV to enable full expressivity. These terms have been submitted to the DPVCG for addition to the vocabulary
- CSM–ROPA requires additional terms to be added to the DPV to reduce the reliance on partial and complex matches for expectations 6.2 "ROPA process" and 6.10 "legitimate interest". These terms will reduce the dependency on partial matches and enhance the expressivity of CSM–ROPA.
- There are many terms (34%) with a partial or complex mapping that will require additional modelling in CSM–ROPA to capture the ICO Accountability Framework perfectly.

Comparison of CSM–ROPA to Manual and Proprietary Privacy Software Accountability Approaches

In this paper, we identified the best practices for supporting the demonstration of regulatory compliance to meet the accountability principle of the GDPR. We have shown that organisations' approaches to meeting the accountability principle are fragmented. It was seen that many organisations have invested in privacy software whilst numerous others continue to rely on manual approaches to compliance. In Sect. 3, we identified the need for tools that support accountability. Section 4 identified the specific requirements these tools must provide, such as the digital exchange of data based on standard semantics and enabling automated accountability compliance verification. In Sect. 7, we demonstrated the expressivity of CSM–ROPA to meet the expectations of the ICO accountability Framework.

We will now evaluate how CSM–ROPA compares to manual approaches and the leading privacy software provider, One Trust [26], in meeting the essential requirements that GDPR accountability tools must have (see Sect. 4.5). We complete this evaluation based upon the critical features required to meet the contemporary challenges of meeting the accountability principle derived from RegTech best practice in Sect. 4 (see Table 5).

When we evaluate each approach to GDPR accountability, we find that all three approaches can record the accountability data necessary to meet their accountability obligations. We find that both manual and the One Trust system do not contain the system requirements to meet best practices. We find that manual solutions cannot support the digital exchange of data nor provide automated compliance verification [10]. Organisations have begun to migrate from manual systems towards privacy software (Fig. 4) over the last years as privacy software gains favour with organisations [30]. Organisations realise that they cannot maintain accountability at scale unless the technology is applied to privacy [34]. Organisations' investment in privacy software has been extensive since 2018 [52]; however, we find that the move to privacy systems brings organisations an alternate set of challenges. Many purchasers have expressed concerns about the "lock-in" effect of buying any privacy tech solution [28] and the lack of agility and flexibility with privacy systems. The One Trust privacy system does not support data exchange between parties (and systems) such as processors and regulators. The ability of privacy systems to interoperate with stakeholders such as regulators, processors and data subjects is vital. This will require an agreement on standard data formats, protocols, and interfaces. Future data protection compliance systems need to agree on common semantic standards and protocols to enable the move to machine-readable ROPA accountability compliance systems to support ROPA compliance. The critical advantage that CSM–ROPA offers over both manual systems and One Trust privacy software is the interoperability of CSM–ROPA. It is designed to act as a mediation lingua franca layer capable of pulling together disparate data sources in heterogeneous

forms to facilitate semantic interoperability for verifiable accountability. It is a new semantic metadata-based approach to describing and integrating diverse data processing activity. CSM–ROPA can enable data gathering from heterogeneous organisational sources such as departments, divisions, and external processors. This information can be collated to assess and document GDPR legal compliance, such as creating a Register of Processing Activities (ROPA).

Conclusions

ROPA creation and maintenance is an area with very little research to date [6, 7]. Our analysis of the ROPA practices of organisations showed that they are greatly challenged in maintaining their ROPA [5]. They continue to rely on spreadsheets and standalone software tools [10] to maintain their accountability data.

The first contribution of this paper is the application of RegTech best practices to resolve a significant GDPR challenge. Previous research has identified the key success factors of RegTech regulatory compliance. Our use case shows that applying these Regtech success factors [11] in a GDPR context can be successful. CSM–ROPA is developed based on these RegTech best practices to assist organisations to support ROPA accountability. The development of the CSM–ROPA semantic model utilising terms agreed by the DPVCG is a step towards the concretisation of agreed terms [29]. We deploy a semantic model to meet a regulator supplied accountability question set to automate regulatory compliance [9]. The regulator's role as an enabler to facilitate digital regulatory compliance is vital [39]. The provision of a detailed accountability tracker question set by the ICO establishes the thresholds that must be reached to demonstrate accountability. This helps the organisation set the objectives of future maturity models as recommended by Laposa [22].

Our second contribution is the demonstration of the expressiveness and effectiveness of CSM–ROPA to facilitate GDPR supported accountability. Our case study identifies that CSM–ROPA could express 98% of the 139 identified unique terms and could fully express nine of the ten expectations in a regulator-supplied accountability framework section. Our analysis finds that CSM–ROPA did not contain the expressiveness to model 3 terms. These terms are "Data Protection Authority", "Data Flow Map", and "Legislation". These terms have been recommended for inclusion in the Data Privacy Vocabulary. Our analysis has identified two regulator expectations, "legitimate interest" and "ROPA process", that could be enhanced from additions to DPV. This would reduce the number of partial matches to DPV and improve the expressivity of CSM–ROPA.

Our third contribution is to identify the key features that systems must possess to assist organisations and show that CSM–ROPA contains the key features to support the digital exchange of accountability data between stakeholders. We show that it can support automated accountability compliance verification.

Our fourth contribution compares CSM–ROPA-based accountability with both manual approaches and a leading proprietary privacy software system. The positive outcome of this research shows that with a small number of new terms added to CSM–ROPA, it is possible to support machine to machine accountability compliance verification for the creation and maintenance of ROPAs and therefore support the demonstration of compliance with the accountability principle.

The key considerations for organisations from this research are that GDPR RegTech offers great possibilities for automated compliance. To achieve this, they must migrate from manual spreadsheets, build their data governance capability, and invest in technology to support compliance.

The key consideration for data protection regulators is that they need to be the enablers of digital compliance. They need to move away from providing manual spreadsheet templates and move to a digital environment where they facilitate the creation of agreed semantics and the development of compliance tools. This will allow organisations and technologists to develop the toolsets to demonstrate accountability.

The limitations to this research are that there has been very little academic research, or external validation in this area. This research will continue with gathering the opinions of the research and practitioner communities. The outcome of this analysis is positive. The outcome of this analysis is positive. The indications are that with a small number of additions to CSM–ROPA, it is possible to use a standardised approach to support the automated demonstration of ROPA accountability to meet the ROPA obligations as determined by a regulator.

Acknowledgements This work is partially supported by Uniphar PLC. and the ADAPT Centre for Digital Content Technology funded under the SFI Research Centres Programme (Grant 13/RC/2106_P2) and co-funded under the European Regional Development Fund. For Open Access, the author has applied a CC BY public copyright licence to any Author Accepted Manuscript version arising from this submission

Funding Open Access funding provided by the IReL Consortium. This work is partially supported by Uniphar PLC. and the ADAPT Centre for Digital Content Technology which is funded under the SFI Research Centres Programme (Grant 13/RC/2106_P2) and is co-funded under the European Regional Development Fund. For the purpose of Open Access, the author has applied a CC BY public copyright licence to any Author Accepted Manuscript version arising from this submission.

Declarations

Conflict of Interest Author Paul Ryan declares that he has no conflict of interest, and author Rob Brennan declares that he has no conflict of interest.

Ethical Standards This research has been conducted in accordance with the DCU Code of Good Research Practice https://www.dcu.ie/sites/default/files/2021-01/144_-_code_of_good_research_practice_rss_v1.2.pdf and DCU is committed to the Irish National Policy Statement on Ensuring Research Integrity in Ireland.

References

1. CNIL. https://www.cnil.fr/en/record-processing-activities. Accessed 15 Feb 2022.
2. International Association of Privacy Professionals (IAPP). The value of investing in well-constructed records of processing activities (iapp.org). https://iapp.org/news/a/the-value-of-investing-in-well-constructed-recordings-of-processing-activities/. Accessed 11 Sept 2021.
3. International Association of Privacy Professionals (IAPP). Trust Arc.: measuring privacy operations. (2019). https://iapp.org/resources/article/measuring-privacy-operations/. Accessed 11 Sept 2021.
4. Ryan P, Pandit HJ, Brennan R. Building a data processing activities catalog: representing heterogeneous compliance-related information for GDPR using DCAT-AP and DPV. In: International Conference on Semantic Systems (SEMANTiCS), Amsterdam, 2021; https://doi.org/10.3233/SSW210043.
5. Castlebridge Register of Processing Activities (2020) https://castlebridge.ie/research/2020/ropa-report/. Accessed 11 Sep 2021.
6. Huth D, Tanakol A, Matthes F. Using enterprise architecture models for creating the record of processing activities (Art. 30 GDPR). In: 2019 IEEE 23rd International Enterprise Distributed Object Computing Conference (EDOC), IEEE. 2019. p. 98–104. https://doi.org/10.1109/EDOC.2019.00021.
7. Martínez-González MM, Alvite-Díez ML, Casanovas P, Casellas N, Sanz D, Aparicio A (2021) OntoROPA Deliverable 1. State of the Art and Ambition.
8. Ryan P, Crane M, Brennan R (2020) Design challenges for GDPR RegTech. In: Proceedings of the 22nd international conference on enterprise information systems—Volume 2: ICEIS, ISBN 978-989-758-423-7; ISSN 2184-4992, pp. 787–795. https://doi.org/10.5220/0009464507870795.
9. Ryan P, Pandit H, Brennan R. A common semantic model of the GDPR register of processing activities (2020).https://doi.org/10.3233/FAIA200876.
10. Ryan P, Crane M, Brennan R. GDPR compliance tools: best practice from RegTech. In: Filipe J, Śmiałek M, Brodsky A, Hammoudi S, editors. Enterprise information systems. ICEIS 2020. Lecture notes in business information processing, vol. 417. Cham: Springer; 2021. https://doi.org/10.1007/978-3-030-75418-1_41.
11. Butler T, O'Brien L. Understanding RegTech for digital regulatory compliance. In: Lynn T, Mooney J, Rosati P, Cummins M, editors. Disrupting finance. Palgrave studies in digital business and enabling technologies. Cham: Palgrave Pivot; 2019. https://doi.org/10.1007/978-3-030-02330-0_6.
12. Ryan P and Brennan R (2021) Demonstrating GDPR accountability with CSM-ROPA: extensions to the data privacy vocabulary. In Proceedings of the 23rd international conference on enterprise information systems—Volume 2: ICEIS, ISBN 978–989–758–509–8; ISSN 2184–4992, pp 591–600. https://doi.org/10.5220/0010390505910600.
13. Bovens M. Analysing and assessing accountability: a conceptual framework. Eur Law J. 2007;13:447–68. https://doi.org/10.1111/j.1468-0386.2007.00378.x.
14. Fieldfisher. Accountability—the enabler to evidencing your compliance under the GDPR. https://www.fieldfisher.com/en/services/privacy-security-and-information/privacy-security-and-information-law-blog/accountability-the-enabler-to-evidencing-your-comp. Last accessed 18 Feb 2022.
15. OECD. Thirty years after the OECD guidelines, (2011). https://www.oecd.org/sti/ieconomy/49710223.pdf.
16. Article 29 Data Protection Working Party. Opinion 3/2010 on the principle of accountability. (2010) 3 (dataprotection.ro). https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp173_en.pdf. Accessed 11 Sep 2021.
17. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data Official Journal L 281, 23/11/1995 P. 0031–0050.
18. Buttarelli G. The EU GDPR as a clarion call for a new global digital gold standard. Int Data Privacy Law. 2016;6:77–8.
19. Korff D, Georges M. The data protection officer handbook (2019). SSRN: https://ssrn.com/abstract=3428957.
20. Centre for Information Policy Leadership. The case for accountability: how it enables effective data protection and trust in the digital society. (2018).
21. International Association of Privacy Professionals (IAPP). GDPR Maturity Framework; 2019. https://iapp.org/resources/article/the-gdpr-maturity-framework/.
22. Laposa T, Frivaldszky G. Data Protection Maturity: an analysis of methodological tools and frameworks. Central Eastern Eur eDem eGov Days. 2020;338:135–47.
23. Information Commissioners Office, https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2021/07/what-s-next-for-the-accountability-framework/. Accessed 11 Sept 2021.
24. Centre for Information Policy Leadership. What good and effective data privacy accountability looks like: mapping organisations' practices to the CIPL Accountability Framework (2021) cipl_accountability_mapping_report__27_may_2020_pdf (informationpolicycentre.com). https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_accountability_mapping_report__27_may_2020_.pdf. Accessed 11 Sept 2021.
25. GDPR Enforcement Tracker - https://www.enforcementtracker.com/. Accessed 18 Feb 2022.
26. IDC Market. Worldwide Data Privacy Management Software Market Shares, 2019: OneTrust Dominates the Competition (2019) (idc.com). https://www.onetrust.com/blog/idc-releases-first-worldwide-data-privacy-management-software-market-shares-report/. Accessed 11 Sept 2021.
27. International Association of Privacy Professionals (IAPP). IAPP-EY annual governance report, 2019. https://iapp.org/news/a/2019-iapp-ey-privacy-governance-report-released-at-psr/. Accessed 11 Sept 2021.

28. International Association of Privacy Professionals (IAPP). 2020 privacy tech vendor report (2021). IAPP Privacy Tech Vendor Report. https://iapp.org/media/pdf/resource_center/2020TechVendorReport.pdf. Accessed 11 Sep 2021.
29. Labadie C, Legner C. Understanding data protection regulations from a data management perspective: a capability-based approach to EU-GDPR. Wirtschaftsinformatik (2019).
30. Future of Privacy Form. Privacy Tech's Third Generation, 2021. FPF-PTA-Report_Digital.pdf. https://fpf.org/wp-content/uploads/2021/06/FPF-PTA-Report_Digital.pdf. Accessed 11 Sep 2021.
31. Cap Gemini, 2019. https://www.capgemini.com/de-de/wp-content/uploads/sites/5/2019/09/Report_GDPR_Championing_DataProtection_and_Privacy.pdf. Accessed 11 Sept 2021.
32. Jakobi T, von Grafenstein M, Legner C, et al. The role of IS in the conflicting interests regarding GDPR. Bus Inf Syst Eng. 2020;62:261–72.
33. Nymity, 2018. https://info.nymity.com/hubfs/GDPR%20Resources/A-Practical-Guide-to-Demonstrating-GDPR-Compliance.pdf.
34. Trust Arc - https://trustarc.com/pdf20/2021_TrustArc_Global_Privacy_Benchmarks_Report.pdf. Accessed 11 Sept 2021.
35. Centre for Information Policy Leadership. Certifications, seals and marks under the GDPR and their roles as accountability tools and cross-border data transfer mechanisms; 2017. https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_gdpr_certifications_discussion_paper_12_april_2017.pdf.
36. Al-Ruithe M, Benkhelifa E, Hameed K. A systematic literature review of data governance and cloud data governance. Pers Ubiquit Comput. 2019;23:839–59. https://doi.org/10.1007/s00779-017-1104-3.
37. Khatri V, Brown CV. Designing data governance. Commun ACM. 2010;53(1):148–152. https://doi.org/10.1145/1629175.1629210.
38. Pandit HJ, O'Sullivan D, Lewis D. Queryable provenance metadata for GDPR compliance. Procedia Comput Sci. 2018;137:262–8. https://doi.org/10.1016/j.procs.2018.09.026 (**ISSN 1877-0509**).
39. Buckley RF, Arner DW, Zetzche DA, Weber RH. The road to RegTech the astonishing example of the European union. J Bank Regul. 2020;21:36–36. https://doi.org/10.1057/s41261-019-00104-1.
40. Arner DW, Barberis J, Buckley RP. The evolution of Fintech: a new post-crisis paradigm. Geo J Int'l L. 2015;47:1271.
41. Arner DW, Barberis J, Buckey RP. FinTech, RegTech, and the reconceptualisation of financial regulation. Nw J Int'l L & Bus. 2016;37:371.
42. Pandit HJ. Representing activities associated with processing of personal data and consent using semantic web for GDPR compliance; Trinity College Dublin, School of Computer Science & Statistics, 2020.
43. Arner DW, Zetzche DA, Buckley RF, Barberis J. Fintech and RegTech: enabling innovation while preserving financial stability. Georgetown J Int Affairs. 2017;18(3):47–58.
44. Bonatti PA, Kirrane S, Petrova IM, et al. Machine understandable policies and GDPR compliance checking. Kunstl Intell. 2020;34:303–15.
45. Debruyne C, Pandit HJ, Lewis D, et al. "Just-in-time" generation of datasets by considering structured representations of given consent for GDPR compliance. Knowl Inf Syst. 2020;62:3615–40.
46. Leone V, DiCaro L. The role of vocabulary mediation to discover and represent relevant information in privacy policies. Legal Knowl Inf Syst. 2020. https://doi.org/10.3233/FAIA200851.
47. Pandit HJ, Polleres A, Bos B, Brennan R, Bruegger B, Ekaputra FJ, Fernández JD, Hamed RG, Kiesling E, Lizar M, Schlehahn E. Creating a vocabulary for data privacy. In: OTM Confederated International Conferences "On the Move to Meaningful Internet Systems" 2019 Oct 21. Cham: Springer; 2019. p. 714–730.
48. Suárez-Figueroa MC, Gómez-Pérez A, Fernández-López M. The NeOn methodology for ontology engineering. In: Ontology engineering in a networked world 2012. Berlin, Heidelberg: Springer; 2012. p. 9–34.
49. De Nicola A, Missikoff M. A lightweight methodology for rapid ontology engineering. Commun ACM. 2016;59(3):79–86. https://doi.org/10.1145/2818359.
50. Sein MK, Henfridsson O, Purao S, Rossi M, Lindgren R. Action design research. MIS quarterly; 2011. p. 37–56.
51. Scharffe F. Correspondence patterns representation (Doctoral dissertation, PhD thesis, University of Innsbruck).
52. Fortune Business Insights. Data Privacy Software Market Size, Growth | report [2022–2029]. 2022; (fortunebusinessinsights.com). https://www.fortunebusinessinsights.com/data-privacy-software-market-105420. Accessed 5 Apr 2022.