GDPR Compliance Tools: Best Practice from RegTech

Paul Ryan[1,2](✉), Martin Crane[1](✉), and Rob Brennan[1](✉)

[1] ADAPT Centre, School of Computing, Dublin City University, Glasnevin, Dublin 9, Ireland
paul.ryan76@mail.dcu.ie, {martin.crane,rob.brennan}@dcu.ie
[2] Uniphar PLC, Dublin, Ireland

Abstract. Organisations can be complex entities, performing heterogeneous processing on large volumes of diverse personal data, potentially using outsourced partners or subsidiaries in distributed geographical locations and jurisdictions. Many organisations appoint a Data Protection Officer (DPO) to assist them with their demonstration of compliance with the GDPR Principle of Accountability. The challenge for the DPO is to monitor these complex processing activities and to advise and inform the organisation with regard to the organisations demonstration of compliance with the Principle of Accountability. A review of GDPR compliance software solutions shows that organisations are being greatly challenged in meeting compliance obligations as set out under the GDPR, despite the myriad of software tools available to them. Many organisations continue to take a manual and informal approach to GDPR compliance. Our analysis shows significant gaps on the part of GDPR tools in their ability to demonstrate compliance in that they lack interoperability features, and they are not supported by published methodologies or evidence to support their validity or even utility. In contrast, RegTech has brought great success to financial compliance, using technological solutions to facilitate compliance with, and the monitoring of regulatory requirements. A review of the State of the Art identified the four success features of a RegTech system to be, strong data governance, automation through technology, interoperability of systems and a proactive regulatory framework. This paper outlines a set of requirements for GDPR compliance tools based on the RegTech experience and evaluate how these success features could be applied to improve GDPR compliance. A proof of concept prototype GDPR compliance tool was explored using the four success factors of RegTech, in which RegTech best practice was applied to regulator based self-assessment checklist to establish if the demonstration of GDPR compliance could be improved. The application of a RegTech success factors provides opportunities for demonstrable and validated GDPR compliance, notwithstanding the risk reductions and cost savings that RegTech can deliver and can facilitate organisations in meeting their GDPR compliance obligations.

Keywords: GDPR · Compliance · Accountability · Data protection officer · RegTech

J. Filipe et al. (Eds.): ICEIS 2020, LNBIP 417, pp. 905–929, 2021.
https://doi.org/10.1007/978-3-030-75418-1_41

1 Introduction

In May 2018, the European Union (EU) introduced the GDPR. This regulation brought about a high level of protection for data subjects, but also a high level of accountability for organisations [1]. The GDPR is a paradigm shift in data protection, towards greater choice and sovereignty for individuals, and more accountability for organisations [2]. The GDPR principle of accountability requires that a data controller must be able to demonstrate their compliance with the regulation (GDPR Recital 74). This requires an organisation "to act in a responsible manner, to implement appropriate actions, to explain and justify actions, provide assurance and confidence to internal and external stakeholders that the organisation is doing the right thing and to remedy failures to act properly" [3].

Organisations can be complex entities, performing heterogeneous processing on large volumes of diverse personal data, potentially using outsourced partners or subsidiaries in distributed geographical locations and jurisdictions. A challenge to complying with the accountability principle of the GDPR for organisations is demonstrating that these complex, dynamic activities and structures are meeting their regulatory obligations. The organisation must implement appropriate policies, procedures, tools and mechanisms to support their accountability practices [3].

Many organisations appoint a Data Protection Officer (DPO) to assist in this process. Bamberger describes the role as "the most important regulatory choice for institutionalising data protection" [4]. In practice the DPO is the early warning indicator of adverse events when processing personal data within the organisation [5]. The DPO must have "professional qualities and, in particular, expert knowledge of data protection law and practices" [GDPR Art 37]. This challenging role requires the DPO to monitor compliance and advise the organisation accordingly. The DPO acts independently of the organisation to assess and monitor the consistent application of the GDPR regulation and to ensure that the rights and freedoms of data subjects are not compromised [6]. The role of DPO encompasses a dynamic motion of policy generation, staff training, business process mapping and review, compliance record keeping, audit, data protection impact assessments, and compliance consultations [5]. The constant pace of business change allied with evolving legal interpretations require constant vigilance on the part of the DPO and create additional challenges for accountability. Fundamentally, it is the organisation, and not the DPO, that must be able to demonstrate that it is meeting the threshold that is the accountability principle as set out in the GDPR [3].

There are many solutions available to DPOs and organisations to help meet this challenge of demonstrating compliance to the accountability principle. We evaluate here the range of available tools, such as: privacy software solutions from private enterprise vendors, maturity models and regulator self- assessment tools. Despite the many GDPR compliance tools available, we highlight that the majority fail to meet the accountability principle. Most are not supported by published methodologies or evidence for their validity or even utility. They lack the ability to integrate or be integrated with other tools and the level of automation and innovation in this space has also been limited.

In contrast, RegTech has emerged as a framework for automating regulatory compliance in the Financial Industry. The "Global Financial Crisis (GFC)" of 2008 prompted financial regulators to introduce new compliance regulations [7], resulting in significant compliance challenges and compliance costs for organisations due to the complexity of these regulations. The digital transformation of data and the assimilation of regulatory compliance provisions into software code [8] to facilitate regulatory compliance has been enabled by developments such as process automation, the digitising of data, the use of semantic methods and machine learning algorithms. RegTech uses such tools to efficiently deliver compliance and risk reports in integrated toolchains. The evolution of RegTech has shown that IT can be used to support automated or semi-automated regulatory monitoring and reporting of compliance [9].

This paper proposes challenges for realising a RegTech approach to GDPR compliance whereby organisations leverage modern information technology to improve the organisational and external visibility of their GDPR compliance level. This approach requires automated data collection from relevant sources throughout the organisation and monitoring via GDPR compliance evaluation functions that could provide interoperable and machine-readable compliance metrics or reports for the organisation, suggested compliance actions and root cause analysis of compliance issues, using agreed data quality standards such as ISO8000. The role of monitoring, analysing and reporting the GDPR compliance status in an organisation is the task of the DPO. A RegTech approach to GDPR compliance could provide the DPO with the ability to track organisational compliance progress, identify areas of compliance weakness and benchmark their performance against other organisations. This would greatly enhance an organisation's ability to demonstrate and improve compliance and thus meet the GDPR accountability requirement.

This paper builds on "Design Challenges for GDPR RegTech", published in ICEIS 2020 [10], and seeks to identify the key success features of RegTech systems and evaluates how these success features could be applied to improve GDPR compliance. It features an updated and detailed review of GDPR compliance tools available to organisations and an enhanced State of the Art review of the key features of RegTech systems. Each of these key features are identified and evaluated to establish how they could be applied to GDPR Compliance.

The rest of this paper is structured as follows: Sect. 2 will discuss the accountability principle and what it means in practice to an organisation and the challenges they face to meet the accountability principle. The role of the DPO, and their part in compliance will be discussed in detail from the perspective of a practising DPO. Section 3 reviews the current approaches to GDPR compliance and critiques the many available offerings such as private enterprise software solutions, maturity models and self-assessment checklists. Section 4 examines RegTech literature to identify the key success features of RegTech systems to understand how RegTech is enhancing compliance using data driven solutions. Section 5 takes these success features and looks at them in a GDPR context to establish the challenges that organisations must face in developing the next generation of GDPR compliance tools. Section 6 will introduce a proof of concept compliance system where a Data Protection Regulators self- assessment checklist has been utilised based on RegTech best practice, to provide a simple efficient method to demonstrate GDPR compliance and meet the requirements of the accountability principle.

2 The GDPR Accountability Principle: A View from the DPO

In this section, this paper will discuss what the accountability principle of the GDPR means to organisations. The paper will look at the challenges that organisations are facing with demonstrating that they are meeting these obligations and it will discuss the role of the DPO in this process.

The Anglo-Saxon word "Accountability" has a broadly understood meaning of how responsibility is exercised and how it is made verifiable [11]. Accountability can be viewed to be an expression of how an organisation displays "a sense of responsibility—a willingness to act in a transparent, fair and equitable way" [12] and "the obligation to explain and justify conduct' [12]. The GDPR accountability principle requires a data controller "implement appropriate and effective measures to put into effect the principles and obligations of the GDPR and demonstrate on request" [11]. In 2018 the Centre for Information Policy Leadership (CIPL) [13] developed accountability-based data privacy and governance programs to encompass the key elements of accountability as described in Fig. 1.

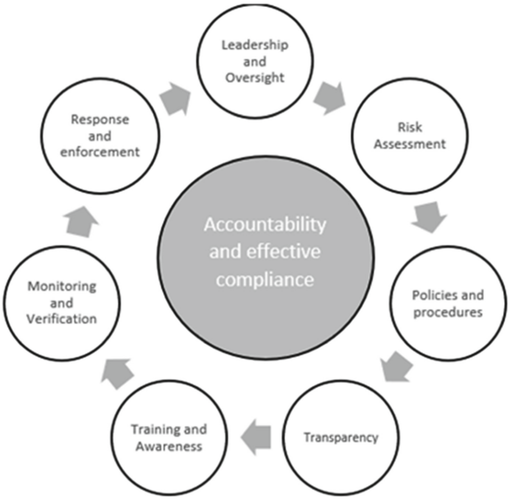


Fig. 1. The accountability wheel–universal elements of accountability [13].

In practice, this can be viewed as "setting privacy protection goals based on criteria established in law, self-regulation and best practices and vesting the organisation with the responsibility to determine appropriate, effective measures to reach these goals" [13]. This is quite a challenging task for a data controller when challenged with a substantial legal text like the GDPR. There is a "lack of awareness of their obligations and duties in relation to personal data protection, it is urgent to define a methodology to be able to comply with the GDPR" [14].

In theory, the GDPR provides for certification methods in article 42 and 43 of the GDPR to assist a controller in demonstrating compliance. However, in practice this has proven to be a challenge for organisations as the European Union has not approved any

Certification body to certify compliance [15]. In fact, there are views being expressed that the GDPR certification process cannot be successful [15].

Many organisations appoint a DPO to assist with their GDPR compliance, however it is important to note that the demonstration of compliance obligations ultimately rests with the controller (organisation) and not the DPO. The role of DPO within the organisation covers a wide range of tasks as prescribed in Article 39 of the GDPR. The main tasks are to monitor, inform and advise the controller or processor regarding compliance with the GDPR, to provide advice such as data protection impact assessments, to provide training and awareness raising and to co-operate with and act as a contact point for the supervisory authority. The DPO must be at the heart of the accountability-based framework [5].

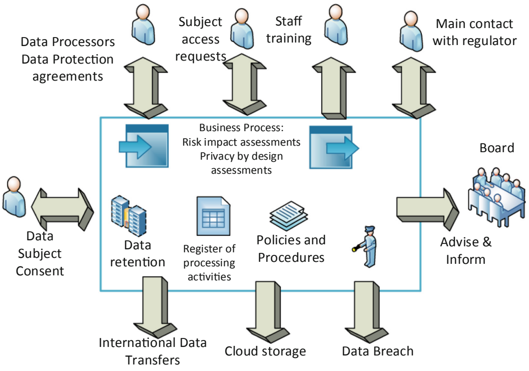


Fig. 2. The breadth and complexity of the role of Data Protection Officer [10].

The role of DPO requires a broad set of skills in GDPR legal compliance, and a detailed knowledge of business processes [5]. The DPO works with numerous stakeholders such as data subjects, employees, processors and regulators and provides consultancy and guidance on business processes. The role involves a broad spectrum of activities from maintaining a register of processing activities to dealing with data breaches, to completing data protection impact assessments. The DPO must have visibility of all activities and monitor and report compliance to the highest level in the organisation (see Fig. 2). The DPO is in essence "privacy on the ground" [16], in that the DPO is the early warning system for GDPR compliance within the organisation [5]. The challenge for the DPO is how to show that the organisation is accountable and how to demonstrate GDPR compliance.

3 An Analysis of Current Approaches to GDPR Compliance

This section discusses the broad range of tools and methods that are available to DPOs to demonstrate the GDPR compliance of their organisation. Each approach will be reviewed and critiqued.

3.1 Private Enterprise Software Solutions

There has been a call for tools and methods to assist organisations in meeting their GDPR compliance obligations [17]. This is being met by large financial investments by venture capital companies with over $500 million invested in privacy related start-ups around the world in 2017 [18]. This has continued into 2020 with significant funding continuing to go into privacy software vendors, such as One Trust $210 m, Ave Point $200 m, Privitar $80 m and BigID $50 m. There are over 304 vendors offering privacy software tools to organisations [19]. This has grown substantially from 2017 when there were 44 such vendors [20] (see Fig. 3).

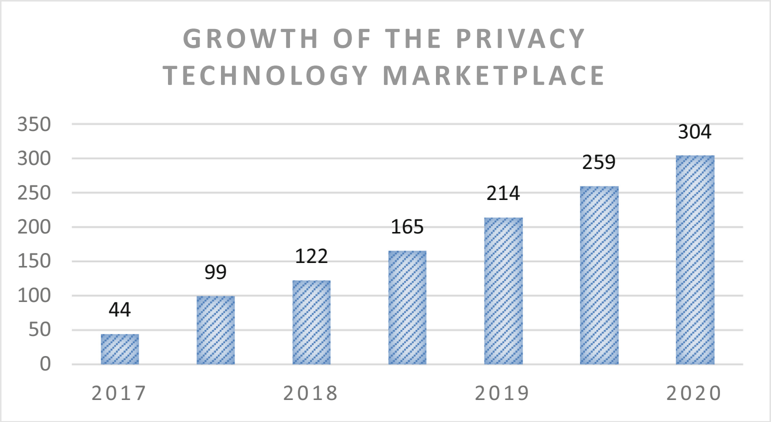


Fig. 3. Growth of the privacy technology marketplace [20].

These software solutions come in many forms ranging from simple questionnaires and templates to solutions that focus on individual aspects of compliance for GDPR such as statistical discovery tools for Data Subject Access Requests (DSAR's) where individuals exercise their right of access to information under Article 15 of the GDPR. The main categories of these privacy tools are as follows [20]:

- Activity Management - control and monitor access to personal data
- Assessment Managers - automate different functions of a privacy program, locating risk gaps, demonstrating compliance
- Consent managers - help organizations collect, track, demonstrate and manage users' consent.
- Data discovery - determine and identify personal data held
- Data mapping solutions - determine data flows throughout the enterprise.
- Data Subject Access Requests (DSAR's) - automation of process
- De-identification pseudonymisation tools
- Secure internal enterprise communications
- Data breach incident response solutions

- Privacy information managers - provide latest privacy laws around the world.
- Website scanning - catalogue cookies

Table 1. Privacy software tools, number of vendors per category [18, 19].

Privacy product category	No. of vendors offering this service 2019	No. of vendors offering this service 2020	Increase 2019 to 2020
Activity monitoring	86	93	+7
Assessment manager	102	118	+16
Consent manager	82	94	+12
Data discovery	91	107	+16
Data mapping	114	140	+26
Data subject requests	–	53	+53
De identification/Pseudonymity	45	55	+10
Enterprise communications	39	54	+15
Incident response	62	86	+24
Privacy information manager	72	96	+24
Website scanning	30	37	+7
Total	248	328	+80

Whilst there are a variety of privacy software solutions being offered by vendors, as displayed in Table 1 "there is no single vendor that will automatically make an organisation GDPR compliant" [18]. In fact, most solutions on offer from private enterprise solution providers cover 3 or less categories, see Fig. 4.

An accountability framework requires a comprehensive approach to compliance across the organisation. Whilst these software solutions go some way towards the demonstration of compliance, the author has identified several weaknesses in these private enterprise software solutions, as follows:

- they are not supported by published methodologies or evidence to support their validity or even utility
- many of these solutions are stand - alone in that they lack inter-operability with other GDPR compliance systems and hence cannot easily be assembled into toolchains providing comprehensive compliance reports and metrics, quality improvement processes or data analytics such as root cause analysis
- they focus on manual or semi-automated assessment approaches that are labour intensive, rely on domain experts and are not driven by quantitative operational data that is increasingly being generated by organisations

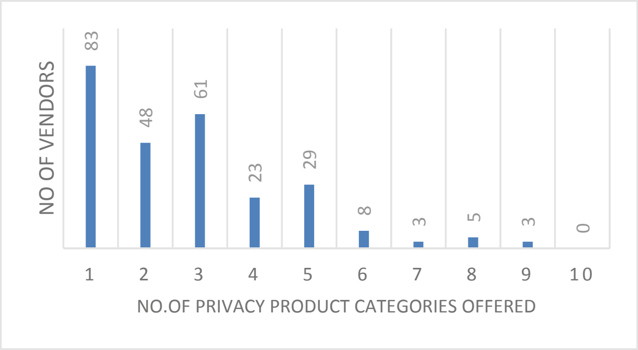


Fig. 4. No. of privacy product categories offered by no. of vendors [18].

- they are created by private enterprise and are based on an interpretation of the regulation, rather than being developed with the input of the regulator.

These solutions offer a starting point for GDPR compliance for an organisation however the lack of academic rigor or formal regulatory input and the inability to connect and build tool chains inhibits these solutions. The use of data driven inputs from heterogeneous sources and the mapping of business processes using agreed semantic standards would improve inputs to the evaluation tool. This would remove subjectivity and improve the quality of the outputs. GDPR compliance software must avoid the "pitfalls of a fragmented Tower of Babel approach." [21]. The 'best-of-breed' software point solution products could be used to feed a global evaluation tool to optimise and organise the outputs using agreed semantics.

3.2 Capability Maturity Models

Capability Maturity Models have been used for compliance monitoring for many years [22]. The American Institute of Certified Public Accountants privacy maturity model [23] was used to gain an understanding of an organisation's privacy compliance standing. It used a set of questions referred to as "generally accepted privacy principles" in the form of 73 measurable criteria. It gauged compliance along an axis of five maturity levels from ad hoc to optimized. The drawbacks of this methodology as a measure of compliance to the GDPR are that it predates the GDPR and would therefore need updating to reflect the new regulation. The more recent International Association of Privacy Professionals (IAPP) Maturity Framework [20] develops a series of checklists built through "collaboration between a team of highly experienced privacy and security professionals, lawyers and regulators." Both solutions provide visualisations of compliance on an axis and are an indicative measure of compliance. However, they do have several drawbacks:

- they are labour intensive and dependent on highly skilled labour/domain experts
- they are prone to human subjectivity, bias and errors
- they are infrequently updated

- the measures chosen utilise a selection of questions and checklists that require academic validation
- an unsuitability as part of an automated process and quality improvement toolchain

Whilst these maturity models are indicative of an organisations GDPR compliance position, the limitations outlined prevent these tools from developing any further without automation. Once automated, the lack of reporting and interoperability standards mentioned in the last section become relevant.

3.3 Accountability Toolkits and Self-assessment Checklists

Several data protection supervisory authorities have provided self-assessment checklists and accountability toolkits to assist organisations to prepare for GDPR. Their purpose is to support organisations to assess whether they have appropriate and effective internal policies, procedures and measures in place to ensure compliance with data protection regulations. These come in the form of a series of questions and checklists and are designed to assist the organisation in checking their compliance level. These toolkits are devised to provide broad coverage of all the principles of the GDPR. Just like maturity models these checklists provide an overview of compliance, however the main drawbacks of these tools for GDPR compliance are that they are fundamentally high-level self-assessments tools and are generic by nature and lack depth. Like maturity models, they rely on qualitative input of users, and they lack input or output interoperability with other solutions. However, the key benefit of these checklists and toolkits are that they have been developed by regulators, unlike maturity models and private enterprise software solutions, which have been developed independently.

3.4 Summary of Findings Regarding GDPR Compliance

This paper has demonstrated that there are several approaches that organisations are taking to GDPR compliance, each with their own weaknesses. The key questions are why is there such different approaches being taken by organisations to compliance? Why are some organisations choosing to rely on spreadsheets and templates, while others develop their own software and more again are investing in privacy tools? Do organisations understand the consequences of non-compliance with the GDPR? In recent analysis

Table 2. GDPR compliance of organisations 2019 [24].

GDPR compliance status	%
Fully compliant	9
Very compliant	36
Moderately compliant	42
Somewhat compliant	12
Not at all compliant	1

from the IAPP [24], the level of GDPR compliance by organisations is still considerably low (see Table 2).

Organisations are being greatly challenged in meeting their compliance obligations as set out under the GDPR, despite the myriad of software tools available to them [24]. Based on our personal experience and conversations with many DPOs and vendors, many organisations are choosing to use manual methods such as spreadsheets to manage their GDPR compliance. They continue to struggle with core GDPR compliance requirements such as Data Protection Impact Assessments (DPIA), Registers of Processing Activities (ROPA) and data inventory mapping (see Table 3). In fact, 76% do not use commercial software tools for carrying out any of these activities [25]. There are many solutions available to organisations to help meet their GDPR compliance, so why are organisations choosing not to implement these?

Table 3. Primary tools used to manage key GDPR compliance processes [25].

Primary tools used to manage key GDPR compliance processes	Data protection impact assessments	Data inventory and mapping	Register of processing activities
Manual /informal	47	45	44
Customised software	20	20	20
Internally developed systems	18	19	21
Governance, risk and compliance software (GRC)	8	10	9
Don’t know	5	2	5
Outsourced	2	4	–
Not applicable	–	–	1

When it comes to another core element of the GDPR, data subject access requests (DSAR’s), organisations are equally challenged. In 2019 DSAR’s were the biggest cause of complaints to the Irish Data Protection Regulator [26]. An analysis of how DSAR’s are addressed by organisations showed only 3% of DSAR’s are automated, and 57% are completely manual (see Table 4) [25]. Despite there being 53 different software vendors (see Table 1) offering solutions to assist organisations, why are organisations failing to meet their compliance obligation in this area? Organisations are facing a steady stream of DSAR’s and are spending significant human capital on satisfying requests [25].

In a similar analysis of the Data protection Impact Assessment (DPIA) personal data risk assessment process, most organisations were found to using manual / informal processes to complete this compliance document. This is also echoed with the Register of Processing Activities (ROPA) where organisations must maintain a recording of their personal data processing activities (see Table 3). These processes are part and parcel of an accountability framework, also mandated by article 30 of the GDPR [25]. Research

Table 4. How Data subject access requests are addressed by organisations [25].

Process used for SAR's	%
Fully automated	3
Partially automated	30
Entirely manual but mature	30
Entirely manual and ad-hoc	27
Still being designed	7
Don't know	2
Have not addressed yet	1

would indicate that organisations are using a variety of manual approaches to the maintenance of this critical record [27]. In fact, Table 3 shows a remarkably similar consistency on the part of the primary compliance tools used by organisations.

Organisations are greatly challenged to meet the accountability principle of the GDPR. The role of the DPO is a challenging one. They must monitor, advise and inform the organisation regarding their GDPR compliance. This is proving to be a significant challenge as many organisations continue to take a manual and informal approach to GDPR compliance [20].

4 An Analysis of the Key Features of RegTech Systems

In this section this paper will conduct a literature review to gain an understanding of what is Regtech, and to identify the key features of a Regtech system.

4.1 Methodology

A search of Google Scholar was conducted using the word "RegTech". The top 12 cited papers were identified, read and reviewed. Our conclusion was that the key success factors which have made RegTech successful are the adoption of developments in technology, the digital transformation of data, agreement on common standards to facilitate interoperability of systems, and the role of financial regulators as facilitators for the automation of regulation (see Table 5).

4.2 What is RegTech?

RegTech can be defined as "the use of technological solutions to facilitate compliance with, and the monitoring of regulatory requirements" [28]. RegTech has played an important role in making regulatory compliance more efficient and effective [21]. RegTech is information technology (IT) that (a) helps firms manage regulatory requirements and compliance imperatives by identifying the impacts of regulatory provisions on business models, products and services, functional activities, policies, operational procedures and controls; (b) enables compliant business systems and data; (c) helps control and manage regulatory, financial and non-financial risks; and (d) performs regulatory compliance reporting [21]. RegTech has evolved to address regulatory challenges in the financial system through innovative technology. It can support the technical handling of large amounts of data, sophisticated analysis and automated data processing within intermediaries as well as between intermediaries and supervisors [29].

Table 5. Literature review - the features of RegTech system.

Publication	Adoption of developments in technology	Digital transformation of data	Common standards and Agreed semantics, interoperability of systems	Role of supervisory authority as enabler/stakeholder
Fintech, RegTech and the reconceptualization of Financial Regulation [30]	✓	✓		✓
Fintech and RegTech Impact on regulators and banks [31]				✓
Fintech and regtech in a nutshell and the future in a sandbox [32]				✓
Adaptive financial regulation and RegTech a concept article on realistic protection for victims of bank failures [33]	✓			✓
Regtech compliance and the technology judgement rule [34]	✓			✓
The emergence of regtech 2.0 from know your customer to know your data [35]	✓	✓		✓

(*continued*)

Table 5. (*continued*)

Publication	Adoption of developments in technology	Digital transformation of data	Common standards and Agreed semantics, interoperability of systems	Role of supervisory authority as enabler/stakeholder
An innovative RegTech approach to financial risk monitoring & supervisory reporting [36]	✓	✓	✓	
RegTech is the new black – the growth of RegTech demand and investment [37]	✓			
Understanding regtech for digital regulatory compliance [21]	✓	✓	✓	✓
RegTech as a response to regulatory expansion in the financial sector [28]	✓	✓	✓	✓
Fintech and RegTech: enabling innovation while preserving financial stability [9]				✓

4.3 Adoption of New Technologies

The first key feature of Regtech is the adoption of new technologies by financial institutions. The Fintech revolution of 2008 has been a key contributor to the success of RegTech [35]. The evolution of Fintech has seen rapid growth and the creation of new opportunities through the application of Big Data, Internet of Things, Artificial Intelligence, machine learning, distributed ledger technology and blockchain, smart contracts and digital identity [29]. This revolution has brought about the creation of many start -up companies that have brought new technologies to help traditional financial entities to deal with the compliance burden placed on them. The advent of regulations such as Know-Your-Customer (KYC) and Anti-Money Laundering (AML) and EU directives such as Markets in Financial Instruments (MiFID and MiFID II), meant that organisations required an investment in technology to meet their compliance obligations.

These complex regulations required automated compliance monitoring and reporting. Organisation can no longer rely on humans to monitor and report complex areas like insider trading and money laundering. The use of technology has enabled the automatic detection, and reporting of irregular activities to a compliance officer, thus reducing the risk of human error in the form of an inattentive staff member. Similarly, tests, help organisations to determine what level of investment advice must be given to a customer based on the results of an automatically processed questionnaire [28]. Again, this solution helps an organisation to reduce errors and meet its legal obligations through process automation. These solutions remove the need for human intervention and make compliance less complex. RegTech tools are being used to leverage data from existing operational information systems and seek to provide agile solutions to improve compliance visibility, through the automation of mundane compliance tasks and reduction of risk to the organisation [28]. The foundation of compliance has been to prevent identify, respond to and remedy risk [38]. RegTech solutions are being developed to meet these regulatory requirements, but also to modernise compliance and generate a measurable value proposition to the organisation. RegTech solutions enhance the basics of compliance through enhanced data integration, the use of automation, predictive analytics and strategic process alignment [38].

4.4 The Digital Transformation of Data

The second key feature of RegTech systems has been the digital transformation of data. The KYC regulation requires an organisation to gather and validate information relating to their customers. Traditionally this was a complex manual process requiring the presentation of documents, recent photographs and proof of identity and address. The digitisation of KYC data has greatly reduced the risk of errors occurring. Similarly, the use of automation and AI to monitor AML regulations to ensure that all transactions undergo constant and scrutinous checks and reviews, has improved regulatory compliance with the prevailing AML guidelines. It entails accessing and evaluating relevant data from various sources, examining historical alerts, and searching for negative information on customers and their counterparties through public domain searches. The use of distributed ledger technology (DLT) has enabled the smooth and seamless sharing of information between financial organisations and regulators [36]. This has resulted in the faster delivery and verification of KYC data and significant savings on time spent on the manual reconciliation of documents.

In 2017, The Economist published an article entitled “The world’s most valuable resource is no longer oil, but data” [39]. This works well when data governance is applied to the data, however upward of 80% of enterprise data today is in an unstructured form [40]. This can be a real challenge and source or risk for an organisation. Unstructured data is any data that resides in emails, files, PDFs or documents that does not have a pre-defined data model. If data is left unstructured it is a significant organisational problem, particularly if it contains sensitive personal data. Historically financial institutions held large amounts of paper-based records. The digital transformation of such data, has facilitated the adaption of new technologies and enabled the organisation to automate processes, gain efficiencies and optimise regulatory compliance.

4.5 Interoperability of Systems Through Common Standards and Agreed Semantics

The third key feature of RegTech systems is the application of semantic standards, through the ability to create machine-readable meta-models that enable data virtualisation across heterogeneous data stores [21]. Data held in siloed, heterogeneous databases can be virtualised, and ontologies and/or predictive analytics/machine learning algorithms and AI applied to automatically classify the data. It can then be used to monitor GDPR compliance, advise on risk and inform stakeholders. When such a knowledge-based model is linked and integrated with a regulatory knowledge base such as legal texts, then it is possible to enable automated regulatory compliance reporting of regulations as part of a business process. It enables an enhanced data-driven approach to the management risk and associated regulatory compliance reporting. "Semantic interoperability ensures that these exchanges make sense— that the requester and the provider have a common understanding of the "meanings" of the requested services and data" [21]. Regtech holds much promise for Regulators and organisation to solve a big problem through collaborative approaches to regulation with a small effort [21]. The full benefits of RegTech will only materialise if the pitfalls of a fragmented Tower of Babel approach are avoided. Semantic standards are the key to all this [21].

4.6 The Role of the Supervisory Authority as an Enabler

The fourth key feature of the success of Regtech has been the role that financial regulators have played, both as a beneficiary and an enabler of RegTech systems. In 2014 Andy Haldane, then Chief Economist at the Bank of England said "I have a dream. It is futuristic, but realistic. It involves a Star Trek chair and a bank of monitors. It would involve tracking the global flow of funds in close to real time in much the same way as happens with global weather systems and global internet traffic. Its centerpiece would be a global map of financial flows, charting spill-overs and correlations." [30].

The regulator now not only has access to periodic or real-time, fine-grained compliance reports, and the incremental improvements in compliance but also promote the design of a regulatory framework able to dynamically adapt to new rules and regulations [32]. The UK Financial Conduct Authority (FCA) has been a leader in this area. They sought to bring innovative technologies that had been successful in Fintech into the regulatory sphere, in a collaborative manner (see Fig. 5). The FCA identified areas of interest and called for tools. They advocated for technology accelerators where FinTech and financial firms were encouraged, in some cases, funding excellent innovations in the use of technology to deliver regulatory compliance and reporting. The regulator sought tool development in areas of interest such as real-time and system embedded compliance/risk evaluation tools, big data techniques, visualisation and automation tools, software integration tools and cloud technologies.

The FCA has hosted 7 Tech Sprints since 2016 to foster innovative and collaborative global financial markets, which brought together financial institutions, academics, regulators and technology companies to want to share experiences and to address key industry problems. An example of the success of these Tech Sprints is where the regulator brought

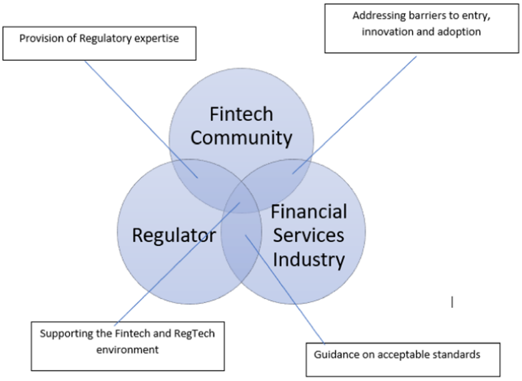

Provision of Regulatory expertise
Addressing barriers to entry, innovation and adoption
Fintech Community
Regulator
Financial Services Industry
Supporting the Fintech and RegTech environment
Guidance on acceptable standards

Fig. 5. A collaborative approach to RegTech fostered by the regulator [41].

the relevant stakeholders together to meet formulate an industry-wide open standards-based approach to regulatory compliance and reporting, which was required by both UK regulators and the financial industry [21]. The Tech Sprint was conducted to prove that standards based RegTech could help automate, and make more efficient and cost-effective, the task of regulatory reporting by financial institutions [21]. The traditional model of masses of documents stored in spreadsheets and PDF documents in servers was challenged. The Tech Sprint proposed solutions such as the use of Natural Language Processing, human and machine-readable rules, machine executable regulatory reports and linked knowledge bases.

4.7 Summary of RegTech Literature Review

The review of the literature identified the key success factors of RegTech systems. The role of the regulator as an enabler featured in almost all literature, and it was the primary success feature for RegTech. Without the regulator's facilitation to make regulations digital, RegTech could not have happened [21]. The adoption of new technologies features widely as a key success factor and is a key enabler to the success of RegTech. The role played by the digital transformation of data and the need for common standards and agreed semantics, Interoperability of systems is less pronounced in the literature, albeit that they are key elements in building RegTech systems. This may be that the literature is more financial in its nature than technology based.

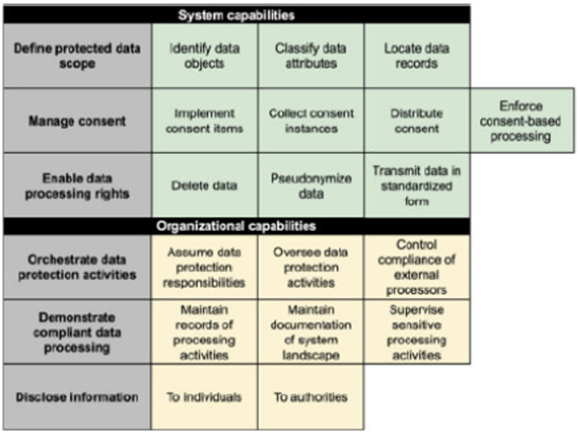
5 RegTech Success Factors Applied to GDPR Compliance

In this section, we take the key success features of RegTech systems as described in Sect. 4 and evaluate how these success features could be applied to improve GDPR compliance. We have identified that the key success features of a RegTech system are the adaption of developments in technology, the digital transformation of data, agreement on common standards to facilitate interoperability of systems, and the role of regulators as facilitators for the automation of regulation. Each success factor will be discussed to establish how they could be applied in a GDPR context to facilitate GDPR compliance.

5.1 Enabling the Digital Transformation of Data

The first requirement for GDPR RegTech is the digital transformation of data. Whilst the Fintech revolution facilitated the digital transformation of data in the financial industry, the same cannot be said for personal data held by non-financial organisations.

Most organisations lack a data governance culture, with the necessary tools and organisational supports. Data governance builds on data management tools and capabilities within the organisation. To date, there is little coverage of data management practices in data protection regulatory compliance in the literature. It is critical that organisations develop and build a dedicated data management capability [2]. Organisations are facing challenges meeting their GDPR obligations due to a lack of common ground between legal and data management domains. Labadie proposes the need for a dedicated data management capability within organisations [2]. This would act as "an abstraction layer between the normative aspects of the regulation, i.e. the regulatory guidelines and compliance requirements (CR), and the concretized compliance requirements (CCR)" [2] to solve organisational problems, (see Fig. 6 for Labadie Capability Model).



System capabilities				
Define protected data scope	Identify data objects	Classify data attributes	Locate data records	
Manage consent	Implement consent items	Collect consent instances	Distribute consent	Enforce consent-based processing
Enable data processing rights	Delete data	Pseudonymize data	Transmit data in standardized form	
Organizational capabilities				
Orchestrate data protection activities	Assume data protection responsibilities	Oversee data protection activities	Control compliance of external processors	
Demonstrate compliant data processing	Maintain records of processing activities	Maintain documentation of system landscape	Supervise sensitive processing activities	
Disclose information	To individuals	To authorities		

Fig. 6. Capability model for GDPR data management [2].

The role that the data management domain plays in facilitating a RegTech approach is seen in Fig. 7. Developing concretized compliance requirements will facilitate compliance demonstration.

Organisations need to have clearly defined data principles, where data is viewed as an asset. The agreed uses of that data must be clearly defined, and the organisation must ensure that the use of data relates positively to the regulatory environment. They need to clearly set out as to what are the organisational behaviors for data quality, who will access the data, how data will be interpreted (metadata), and how long it will be retained [42] An organisation processing personal data must be able to locate and categorise all personal data held that they hold (data catalogs plus data classification). They need to understand the level of sensitivity of the data processed, where it is stored, who is the owner of the data, who has access to the data, how data evolves through a lifecycle, what lifecycle stage it is at and how long the data is retained for.

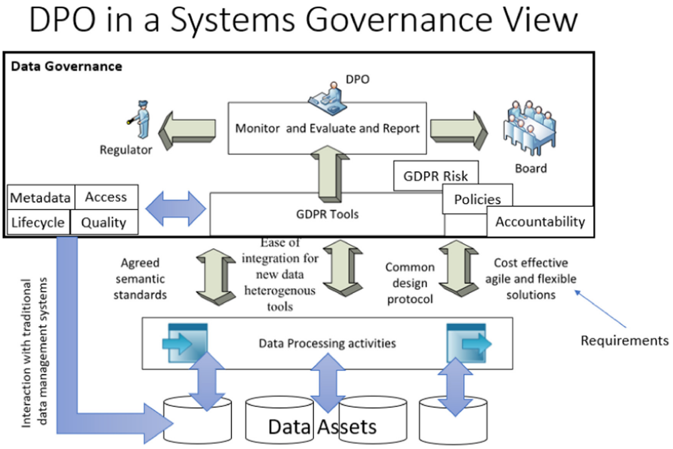

DPO in a Systems Governance View
Data Governance
DPO
Regulator
Monitor and Evaluate and Report
Board
GDPR Risk
Policies
Accountability
Metadata
Access
Lifecycle
Quality
GDPR Tools
Interaction with traditional data management systems
Agreed semantic standards
Ease of integration for new data heterogenous tools
Common design protocol
Cost effective agile and flexible solutions
Requirements
Data Processing activities
Data Assets

Fig. 7. Areas where IT will have to expand to support GDPR RegTech.

The GDPR is concerned with the protection of personal data that of a living individual. This type of data can be found in many guises within an organisation and can stretch to a substantial amount of data points. Such personal data can be found in many forms from HR files to CCTV images to internet browsing history. The challenge that organisations are facing about personal data is locating, classifying and cataloging this data i.e. creation of appropriate metadata to enable management of the personal data. The organisation must create management policies to enable machine-interpretation of data so that it is possible to automate business operations and enforcement. Effective digital policies require machine-readable models of the organisation, its people and resources, its data processing activities and so forth. Essentially this means having a "digital twin" (or data model) of the organisation and other relevant stakeholders like customers and the regulator. Building these models is not enough, organisations also need data governance, management and processing platforms that can interact to track data, processing activities and enforce policies. This would enable the automated creation of accountability logs with strong auditing capabilities. Once such systems are in place then value-added data governance and compliance tools can be built for areas such as risk management, data quality management, data value assessment, organizational change management and decision support tools.

5.2 Adoption of Developments in Technologies to GDPR Compliance

The second requirement for GDPR RegTech is the adaption of new technologies in the same manner that has been at the forefront of the successes of RegTech. A GDPR Regtech solution will require the same approach to new technology to facilitate efficient and effective compliance. The Fintech 3.0 revolution [43] which began in 2008 brought about the implementation of Big Data collection and analytics techniques, machine learning, Natural Language Processing (NLP), Artificial Intelligence (AI), cloud technology, devops (continuous development), Distributed Ledger tech, software integration tools and many other technologies in the financial industry. The cost of compliance and the need for agile solutions brought about the speedy and effective implementation of such new technologies. A RegTech approach to GDPR would require organisations to implement such technologies in a GDPR environment. The transformative nature of technology [30] enjoyed by RegTech can be achieved in the GDPR environment through by a new approach to technology at the nexus of data, digital identity, and regulation.

5.3 Agreement on Common Standards/Agreed Semantics for Personal Data Processing

The third requirement for GDPR RegTech is the need to make personal data interoperable between systems. Whilst the digital transformation of financial data in RegTech has facilitated the application of technology to this data, this may be more challenging in a GDPR environment where large amounts of data is held in manual forms (refer to Table 3 and 4). The semantic modelling of GDPR business processes would be a great benefit to an organisation and provide for machine-readable and interoperable representations of information that can be queried and verified based on open standards such as RDF, OWL, SPARQL, and SHACL [27, 44]. When these models are combined with legal knowledge bases, they become very useful for compliance evaluation and monitoring, which can help to harmonise and facilitate a common approach between legal departments and other stakeholders to the identification of feasible and compliant solutions around data protection and privacy regulations [2]. There has been progress to develop "Core Vocabularies', maintained by the Semantic Interoperability Community (SEMIC), that provide a simplified, reusable and extensible data model for capturing fundamental characteristics of an entity in a context-neutral fashion [45] in this area to foster interoperability. This work continues to be built on through the development of the W3C Data Privacy Vocabulary (DPV) and the PROV-O Ontology [45].

5.4 Data Protection Supervisory Authorities as an Enabler

The fourth requirement for GDPR RegTech is the need for proactive regulators, who will work with organisations to automate regulation and make compliance easier to achieve. The role of supervisory authority has been a major driving force in the success of RegTech, however Data Protection regulators are lagging behind their financial counterparts. There has been some effort by data protection regulators to make the business of compliance easier through the provision of guidance documents, self-assessment checklists and templates, however this remains far removed from the success of RegTech. Whilst each GDPR regulator must apply the GDPR consistently (GDPR recital 135) there have been very little in the form of a unified approach to technical solutions to facilitate GDPR compliance. In fact, an analysis of ROPA templates provided by regulators showed that there were inconsistencies in templates where some templates had as little as 12 fields whereas others had 43 fields. [27]. Perhaps there is a role for the European Data Protection Board (EDPB) as an independent European body, which contributes to the consistent application of data protection rules throughout the EU, and promotes cooperation between the EU's data protection authorities; this may be the way forward here. There have been a number of positive initiatives such as the development of the Internet Privacy Engineering network (IPEN), which promotes and advances the state-of-the-art of privacy engineering among regulators, academia, open source and business development, and other individuals who are committed to finding engineering solutions to privacy challenges. The over-all objective is to integrate data protection and privacy into all phases of the development process, from the requirements phase to production. The EDPB has also released open source software known as the “Website evidence collector” [46], which is a step in the right direction. There have been positive moves by the UK regulator (ICO) to develop sandboxes to work with innovators in privacy technology, however this is very much in the early days. For GDPR RegTech to be successful GDPR regulators need to move towards a symbiotic relationship with technology innovators and organisations processing personal data to develop open source compliance tools, digital regulations, sandboxes [9] and tech sprints. This would greatly accelerate the successes of GDPR RegTech solutions.

5.5 Summary

The key success features of RegTech systems are the adaption of developments in technology, the digital transformation of data, agreement on common standards to facilitate interoperability of systems, and the role of regulators as facilitators for the automation of regulation. If GDPR RegTech is to be realised it will require “a carefully tailored design of the technology, a joint effort of the regulators and the private sector and some shifts in corporate thinking [34]”. Many Organisations have begun to invest or develop technology to facilitate compliance, whilst many others continue to rely on spreadsheets. The need for common ground between the legal and data management domain, would facilitate the digital transformation of data and be a major step towards digital compliance. Data Protection regulators have a major role to play as an enabler and facilitator of digital transformation of regulation and the formulation on common standards and agreed semantics for personal data processing.

6 Proof of Concept: An Evaluation Tool for GDPR Compliance

In this section we describe a prototype GDPR high-level evaluation tool that has been developed based upon the developments in RegTech, outlined in Sect. 5. The tool is an open-source high level GDPR compliance evaluation methodology that has been based on a self-assessment checklist created by a data protection regulator. It has been developed to measure the GDPR compliance level in an organisation. The evaluation tool was developed from the Irish Data Protection Commission self- assessment checklist [47] which segmented the GDPR into 8 regulatory sections and posed 54 questions in total. The tool is designed to be a layered information delivery system that provides information and insights so that the DPO can measure, monitor and manage business performance more effectively, and address accordingly [48].

The evaluation tool provides three layers of data as displayed in Fig. 8. The top level being a graphical overview of compliance for monitoring and reporting purposes, the second layer being the dimensional data that provides a view of each aspect of the GDPR and the final layer that being the detail of each GDPR compliance area.

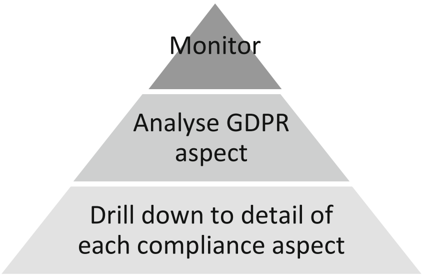


Fig. 8. GDPR evaluation dashboard overview [48].

It is planned that the tool will use the W3C Community group's data protection vocabulary [49] to describe the context using explicit semantics and the W3C Data Cube vocabulary to represent the time series of measurements across the different GDPR aspects or dimensions [50]. This development involved taking the self-assessment checklist and transforming it into an evaluation tool which was populated by a sample organisation each month for six months in total. The overall GDPR compliance monthly score for the organisation for each month is displayed in Fig. 9. This information gives the DPO a high-level view of compliance for the organisation.

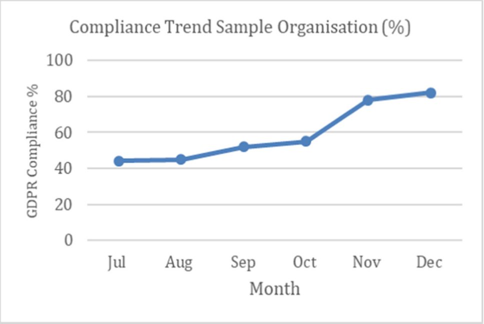


Fig. 9. Compliance trend for sample organisation [10].

The results from the evaluation tool can be also viewed by GDPR regulatory section to analyse how the organisation is performing in the various aspects of GDPR compliance, thus providing enhanced visibility to the DPO. In Table 6 the organisation is fully compliant in accuracy and retention but is only 50% compliant regarding data breaches. The data can be examined to another sub-level to provide the detail by GDPR aspect. Table 7 breaks out the Data Breach aspect and provides the granularity that a DPO needs to provide feedback to the controller to drive actions and improve the compliance of the organisation.

In the sample organisation the DPO can identify the non-compliant areas as identified in Table 3 and take the necessary actions to resolve.

Table 6. Compliance score per regulatory area [10].

GDPR section	Compliant %
Personal data	67%
Data subject rights	40%
Accuracy and retention	100%
Transparency requirements	100%
Other data controller obligations	83%
Data security	100%
Data breach	50%
International data transfers	100%
Total score	82%

Table 7. Non-compliance results for data breach [10].

Data breach section	Areas of failure
Are plans and procedures regularly reviewed?	Non-compliant
Are all data breaches fully documented?	Non-compliant
Are there cooperation procedures in place between data controllers, suppliers and other partners to deal with data breaches?	Non-compliant

This approach has demonstrated the use of a RegTech approach to GDPR compliance using a simple cost-effective method. It has utilised questions that have been created by regulatory authorities themselves so they could serve as a strong platform for the assessment of compliance. The evaluation tool meets the requirement of being comprehensive in that it covers the breadth of the GDPR and is informative in that it provides specific scores into GDPR areas requiring focus. The evaluation process is repeatable in that it can be run at intervals to generate compliance trends. The results yielded specific and relevant scores that can be used to drive corrective actions. The use of data driven inputs from heterogeneous sources and the mapping of business processes into the evaluation tool using agreed semantic standards would remove qualitative user inputs and would improve inputs to the evaluation tool. This would remove subjectivity and improve the quality of the outputs.

7 Conclusions

The accountability principle of the GDPR requires organisations be accountable for the demonstration of their compliance with the regulation. We have seen that the DPO is greatly challenged to monitor GDPR compliance as each of the available GDPR compliance tools, have their shortcomings. Our research question asked could a Regtech approach to the GDPR be successful? We reviewed RegTech literature and identified that the success features of a RegTech system are, the adoption of developments in technology, the digital transformation of data, agreement on common standards to facilitate interoperability of systems, and the role of regulators as facilitators for the automation of regulation. The application of these RegTech key success factors to the GDPR has already begun, in that organisations are moving towards technology as a solution to their GDPR compliance. Some of these organisations are acting independently and developing their own compliance software tools, whilst others are investing in privacy software or manually managing their compliance on spreadsheets. Organisations need a dedicated data management capability to build common ground between the legal and data management domains, to facilitate the digital transformation of data. GDPR Regulators have lacked the proactivity of financial regulators in the facilitation of automated digital compliance. This lack of leadership has resulted organisations facing the "pitfalls of a fragmented Tower of Babel approach" [21]. The role of the supervisory authority was identified as a key enabler and facilitator, for RegTech, however GDPR Regulators have been quite slow to take a similar role in comparison to financial regulators. We have shown that the use of technology to improve compliance monitoring and reporting can be achieved when flexible, agile, cost effective, extensible and informative tools are combined, particularly when the regulator facilitates digital compliance. The failure of GDPR regulators to actively promote digital regulatory compliance standards is resulting in slow progress towards digital compliance.

A proof of concept was conducted to demonstrate the application of some of these RegTech approaches to GDPR Compliance. A GDPR compliance tool was developed from a regulator supplied self-assessment tool to monitor and analyse organisational compliance that yielded a GDPR compliance output for an organisation. The compliance report that was generated from the evaluation tool can be used to identify GDPR areas where the organisation is not compliant, to trend their progress towards GDPR compliance over time and to benchmark performance versus other organisations. The DPO can use the results to direct resources to areas of non-compliance and improve their score, thus reducing the risk of GDPR fines. We have shown that a RegTech approach to GDPR can enable an organisation to meet its obligations to comply with the accountability principle.

Acknowledgements. 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) and is co-funded under the European Regional Development Fund.

References

1. Buttarelli, G.: The EU GDPR as a clarion call for a new global digital gold standard. Int. Data Priv. Law, 77–78 (2016)
2. Labadie, C., Legner, C.: Understanding Data Protection Regulations from a Data Management Perspective: A Capability-Based Approach to EU-GDPR (2019)
3. Felici, M., Koulouris, T., Pearson, S.: Accountability for Data Governance in Cloud Ecosystems (2013)

4. Bamberger, K., Mulligan, D.: Privacy on the Ground: Driving Corporate Behaviour in United States and Europe, p. 204. MIT Press (2015)
5. Drewer, D., Miladinova, V.: The canary in the data mine. Comput. Law Secur. Rev. **34**, 806–815 (2018)
6. Eur. Union.: Charter of Fundamental Rights of The European Union. Official J. Article 8, (2012)
7. Johansson, E., Sutinen, K., Lassila, J., Lang, V., (eds.) Martikainen M., Lehner, OM.: RegTech-A Necessary Tool to Keep up with Compliance and Regulatory Changes? (2019)
8. Bamberger, K.: Technologies of compliance: Risk and regulation in a digital age. Texas Law Rev. (2009)
9. Arner, D.W., Zetzche, D.A., Buckley, R.F., Barberis, J.: Fintech and RegTech: enabling innovation while preserving financial stability. Georgetown J. Int. Affairs **18**, 47–58 (2017)
10. Ryan, P., Crane, M., Brennan, R.: Design Challenges for GDPR RegTech, ICEIS 92), pp. 787–795 (2020)
11. Article 29 Data Protection Working Party.: Opinion 3/2010 on the Principle of Accountability (2010)
12. Boven's, M.: Analysing and Assessing Accountability: A Conceptual Framework (2007)
13. Centre for Information Policy Leadership.: The Case for Accountability: How it Enables Effective Data Protection and Trust in the Digital Society (2018)
14. Da Conceicao Freitas, M., Silva M.: GDPR compliance in SME's: There is much to be done. J. Inf. Syst. Eng. Manage. (2018)
15. Lachaud, E.: Why the certification process defined in the General Data Protection regulation cannot be successful? Comput. Law and Secur. Rev. **32**, 814–826 (2016)
16. Heimes, R.: Top 10 operational impacts of the GDPR: Part 2 – The mandatory DPO (2016)
17. Piras, L., et al.: DEFeND architecture: a privacy by design platform for GDPR compliance. In: Gritzalis, S., Weippl, E.R., Katsikas, S.K., Anderst-Kotsis, G., Tjoa, A.M., Khalil, I. (eds.) TrustBus 2019. LNCS, vol. 11711, pp. 78–93. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-27813-7_6
18. IAPP: 2018 Privacy Tech Vendor Report (2018)
19. IAPP: 2020 Privacy Tech Vendor Report (2020)
20. IAPP: 2019 The GDPR Maturity Framework. https://iapp.org/resources/article/the-gdpr-maturity-framework/. Accessed 31 July 2020
21. Butler, T., O'Brien, L.: Understanding RegTech for Digital Regulatory Compliance, Disrupting Finance (2019)
22. Humphrey, W.S.: Three process perspectives: Organizations, teams, and people. Ann. Softw. Eng. **4**, 39–72 (2002)
23. The American Institute of Certified Public Accountants (AICPA). Privacy Maturity Model (2011)
24. IAPP-EY annual privacy governance (2019)
25. IAPP – Trust Arc: Measuring Privacy Operations (2019)
26. Data Protection Commission. Annual Report 2020, p. 13 (2020)
27. Ryan, P., Pandit, H., Brennan, R.: Towards a Semantic Model of the GDPR Register of Processing Activities (2020)
28. Colaert, V.: RegTech as a response to regulatory expansion in the financial sector (2017)
29. Buckley, R.F., Arner, D.W., Zetzche, D.A., Weber, R.H.: The road to RegTech the astonishing example of the european union. J. Banking Regul. **21**, 36 (2020)
30. Arner, D., Barberis, J., Buckley, R.: FinTech, RegTech, and the Reconceptualization of Financial Regulation (2016)
31. Anagnostopoulos, I.: Fintech and RegTech impact on regulators and banks. J. Econ. Bus. **100**, 7–25 (2018)

32. Arner, D., Barberis, J., Buckley, R.: Fintech and RegTech in a Nutshell and the Future in a Sandbox. CFA Institute Research Foundation (2017)
33. Baxter, L.G., Duke, L.J.: Adaptive Financial Regulation and RegTech: A Concept Article on Realistic Protection for Victims of Bank Failures (2016)
34. Packin, N.G., Chi-Kent, L.: RegTech, Compliance and the Technology Judgement Rule (2018)
35. Arner, D.W., Barberis, J.N., Buckley, R.P.: The emergence of RegTech 2.0: From know your customer to know your data. J. Financ. Transform. **44**, 79 (2016). UNSW Law Research Paper No. 17-63. http://dx.doi.org/10.2139/ssrn.3044280
36. Kavassalis, P., Stieber, H., Breymann, W., Saxton, K., Gross, F.J.: An innovative RegTech approach to financial risk monitoring and supervisory reporting. J. Risk Finan. **19**(1), 39–55 (2018). https://doi.org/10.1108/JRF-07-2017-0111
37. Larsen, K., Gilani, S.: RegTech is the new black - the growth of RegTech demand and investment. J. Fin. Transform. Capco Inst. **45**, 22–29 (2017)
38. Deloitte.: Compliance Modernization is no Longer Optional https://www2.deloitte.com/lu/en/pages/strategy-operations/articles/compliance-modernization-no-longer-optional.html. Accessed 31 July 2020
39. The Economist: The World's Most Valuable Resource Is No Longer Oil, But Data (2017)
40. Vellingiri, J., Basser, K.K.: Data Management and Big Data Analytics: Data Management in Digital Economy (2019). https://doi.org/10.4018/978-1-5225-5137-9.ch001
41. Financial Conduct Authority: Call for Input: Supporting the development and adoption of RegTech (2015)
42. Khatri, V., Brown, C.V.: Designing Data Governance. Commun. ACM **53**(1) (2010)
43. Arner, D., Barberis, J., Buckley, R.: The Evolution of Fintech: A New Post-Crisis Paradigm? (2015)
44. GDPR Data Interoperability Model. Harshvardhan J. Pandit, Declan O'Sullivan, Dave Lewis (2018)
45. Pandit, H.J.: Representing Activities associated with Processing of Personal Data and Consent using Semantic Web for GDPR Compliance (2020)
46. https://joinup.ec.europa.eu/solution/website-evidence-collector/about
47. Data Protection Commission. https://www.dataprotection.ie/en/organisations/self-assessment-checklist
48. Eckerson, W.: Performance Dashboards: Measuring, Monitoring, and Managing Your Business, 2nd edition (2010)
49. Pandit, H., et al.: Creating a vocabulary for data privacy. In: Panetto, H., Debruyne, C., Hepp, M., Lewis, D., Ardagna, C.A., Meersman, R. (eds.) OTM 2019. LNCS, vol. 11877, pp. 714–730. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-33246-4_44
50. Cyganiak, R.: The RDF data cube vocabulary. https://www.w3.org/TR/vocab-data-cube/. Accessed 31 July 2020