DATA PROTECTION MATURITY: AN ANALYSIS OF METHODOLOGICAL TOOLS AND FRAMEWORKS

Tamás Laposa[1] and Gáspár Frivaldszky[2]

DOI: 10.24989/ocg.338.11

Abstract
This paper discusses the maturity of data protection and privacy measures in order to develop a better understanding of the importance and impacts of this domain.

The practical relevance of this topic is that the General Data Protection Regulation provides that data controllers in EU Member States shall comply with uniform data protection rules. Even though European legislation sets detailed requirements for data controllers, the implementation of appropriate technical and organisational measures can be realised at different levels of maturity. Based on the analysis of the pertinent literature, various maturity models are available to assess privacy policies, but GDPR requirements are addressed just partially. The exploration of the issue of maturity offers a new relevant research opportunity to assist data controllers in finding the appropriate methodology for the assessment and further development of their data protection measures.

This paper has three main objectives. First, to systematically review the relevant literature on the issue of maturity. Second, to analyse the relevant maturity models and their main methodological elements. Third, to make suggestions for a new specific model focusing on GDPR requirements.

1. Introduction

Rapid technological developments and globalisation have brought new challenges for data protection[3]. Technology has transformed both the economy and social life and should further facilitate the free flow of personal data within the Union and the transfer to third countries and international organisations, while ensuring a high level of data protection. [7, Recital (6)] Technological changes bring about the transformation of public sector services and the appearance of new and more sophisticated e-government solutions. Technology allows both private companies and public authorities to make use of personal data on an unprecedented scale.

In order to ensure a consistent level of protection for natural persons throughout the Union and to prevent divergences hampering the free movement of personal data within the internal market, the European Commission drew up and adopted a regulation to provide legal certainty and transparency for economic operators and to provide natural persons in all Member States with the same level of legally enforceable rights. [7, Recital (13)] The above regulation (Regulation 679/2016 of the European Parliament and of the Council) became known as the General Data Protection Regulation (hereinafter referred to as 'GDPR') in the scientific discourse.

[1] Private individual

[2] Private individual

[3] 'personal data' means any information relating to an identified or identifiable natural person ; [GDPR, Article 4]

According to GDPR controllers[4] shall implement appropriate technical and organisational measures to ensure that data processing[5] complies with the prescribed data protection requirements. These measures shall take into account the nature, scope, context and purposes of processing as well as the risks for the rights and freedoms of natural persons. [7, Article 24]

GDPR compliance can be described as a journey. The applied measures shall be reviewed and updated as the technological and legal environment changes. Besides, GDPR applies a risk-based approach to data processing activities, namely controllers shall comply with legal obligations according to the level of risks. [6] According to the approach of this article the progress made along this journey and the scalability of obligations could be best described with the methodology of maturity models. Maturity models can be used to assess both the completeness (whether a controller has implemented all elements of a privacy program), and readiness (to what degree the measures applied are effective) of a privacy program. [23] These models are methodological tools for the preparation for privacy certification as well. Based on the analysis of the pertinent literature, only a few researchers have nevertheless addressed the problem of privacy maturity.

This paper reviews the methodology of maturity models and compares twelve models in the domain of privacy based on their main methodological elements. The results and findings of the analysis pave the way for further research and the paper makes suggestions for a new GDPR-specific model.

2. The methodology of maturity models

Lahrmann et al. define maturity as “the state of being complete, perfect or ready” where this stage can be achieved by an evolutionary progress from an initial stage to an end stage. [13] The concept of maturity measurement was published by the Software Engineering Institute (SEI) – Carnegie Mellon with the introduction of the Capability Maturity Model (CMM). [21] Reviewing the relevant papers, we found that more than a hundred different models have been created since for various domains. [2] In this section, the article discusses the role and typology of maturity models to develop a better understanding of their methodological background.

2.1. The role of maturity models

Caralli et al. define a maturity model as a set of characteristics, attributes, indicators or patterns representing progress in a particular domain or discipline. These models help organisations to evaluate and benchmark their practices, processes and methods against a clear set of standards or best practices of the given domain or discipline. Organisations can apply maturity models to define their current level of maturity and then determine the expected path of improvement. [5] According to *Bruin et al.,* maturity models are evaluative tools to assess and increase the maturity (competency, capability, level of sophistication) of a specific domain on the basis of an agreed set of criteria. [4]

A maturity model represents a desired evolution path for organisations or processes as discrete stages (a sequence of maturity levels). [2] The most frequently-used way of evaluation is a five-point Likert scale where Level 5 represents the highest level. [4] *Levels* represent the transitional states in the model; they describe evolutionary steps. *Attributes* are the core model components measured on each

[4] ‘controller’ means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; [GDPR, Article 4]

[5] ‘processing’ means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means [GDPR, Article 4]

level. They are based on best practices or standards expressed as indicators or processes. In many models attributes are grouped together into so called *process areas or domains*. [5]

In the model, organisations or processes advance between an initial stage and a final stage which represents total maturity. During this advancement the capabilities of the organisations or process performance progresses evolutionarily. The maturity model is a tool to determine the position of the organisation or the process on the evolution path by providing criteria and characteristics to be fulfilled to reach a particular maturity level. [2]

2.2. Typology of maturity models

Reviewing the relevant literature, it can be noticed that maturity models focus on different maturity factors such as *process maturity* (to which extent a specific process is defined, managed, measured, controlled, and effective), *object maturity* (level of sophistication of a piece of software) and *people capability* (ability of knowledge creation and proficiency enhancement). From the perspective of maturity factors models can be one-dimensional or they can address different factors. [15]

As to their nature, maturity assessment models can be descriptive, prescriptive or comparative. A *descriptive model* is simply used for the assessment of the current state of play, i.e. the 'as-is' situation without any provisions for further improvement of maturity. A *prescriptive model* focuses on maturity improvement and enables the elaboration of an improvement roadmap for a specific domain. A *comparative model* enables benchmarking across different organisations, industries or regions. [4]

Concerning the structure of maturity stages, two models types can be distinguished (*fixed-level* and *focus area maturity models)*. Fixed-level models consist of generic maturity levels and they are well-suited to the assessment and benchmarking of organisations. In many cases, these models cannot capture the interdependencies of the different processes that need to be improved in a specific domain. Focus area maturity models identify focus areas that need to be developed and the distinct focus areas have a different evolution path i.e. the number of development stages may vary from area to area. These models enable a more balanced and incremental improvement by helping organisations to address the complexity of the factors determining the effectiveness of a specific domain. [3]

3. The specifics of GDPR

Privacy regulations respond to the challenges and changes of the technological environment. The legislation seeks to promote the implementation of data protection principles and the enforcement of the rights of natural persons in all continents. Nonetheless, different regulations are characterised by specific features, so this section provides an overview of the unique dimension of GDPR.

GDPR expressly commits itself to have a risk-based approach to privacy compliance. Trying to align with data protection rules, controllers have to consider the likelihood and severity of the risk to the rights and freedoms of the data subject taking into account the nature, scope, context and purposes of processing [7, Recital (76); Article 39]. However, the road to privacy compliance is rarely interrupted by Y road junctions; answers to challenges are not black and white. Each organisation should define the acceptable level of risk that it considers appropriate across the breadth of its business. [10, p7] Given the wide range of the possible answers to privacy challenges, risks can vary in case of different organisations and data processing activities according to the risk appetite[6] of controllers and processors. It is reasonable to suppose that the level of compliance can be measured alongside the risks identified.

An example of the risk-based approach is the data protection impact assessment methodology which is a unique requirement of GDPR. Where processing operations are likely to result in a high risk to the rights and freedoms of natural persons, the controller shall carry out an impact assessment to evaluate, in particular, the origin, nature, particularity and severity of that risk. Based on the above assessment, the controller shall design and implement appropriate measures to mitigate the identified risk. [7, Recital (84)] Following the risk-based approach, another unique requirement of GDPR is the establishment of special rules for the processing of special categories of personal data[7].

GDPR states that the protection of natural persons should be technologically neutral and should not depend on the techniques used. [7, Recital (15)] It is conceivable to hypothesize that European legislators intended to create a long-lasting regulation in the quickly developing domain of data protection and sought to prevent creating a serious risk of circumvention.

Probably the most typical and thus unique characteristic of GDPR is the identification of the legal basis. The regulation defines a closed list of legal bases which shall be identified in case of each data processing activity carried out. Besides, controllers shall inform data subjects of the legal bases of activities in their privacy notice. Finding the right legal basis and preparing the relevant documents in accordance with the accountability principle (the “super principle”[8] of GDPR) is one of the most time-consuming tasks on the road to GDPR-compliance. Following the principle of accountability, records of processing activities constitutes the basis of GDPR compliance and its obligatory content is established in the regulation. Some kind of data inventory, data mapping or data register is usually a part of privacy compliance programs and regulations worldwide. Meanwhile some elements of the records, like transfers of personal data to a third country or the description of the purposes of the processing, are typically European.

4. Privacy and data protection maturity models

This section presents the main objectives and the maturity levels of twelve models from different continents. The list of models is the result of a search carried out in different scientific databases (*Sciencedirect, Google Scholar, Researchgate, Taylor and Francis*) and among the documents of different privacy consulting firms. Although the issue of privacy maturity is discussed in the pertinent scientific literature, the majority of the examined models do not stem from academic sources.

Model 1. - AICPA/CICA Privacy Maturity Model (AICPA PMM): this model provides entities with a tool to assess their privacy management activity against criteria based on the list of Generally Accepted Privacy Principles (GAPP). GAPP convert complex privacy requirements into a single privacy objective supported by 10 privacy principles. In the model, principles are backed by 73 attributes that form the basis for the effective management of privacy risks and compliance. [1]

[6] The ISO 31000 risk management standard refers to risk appetite as the "Amount and type of risk that an organization is prepared to pursue, retain or take".

[7] GDPR prohibits the processing of the special categories of personal data by default. They can be processed under special circumstances detailed in Aticle 9

[8] The controller shall be responsible for, and be able to demonstrate compliance with the rules of GDPR; Article 5 (2)

Level	Level name	Description
1st	ad hoc	procedures are generally informal, incomplete, and inconsistently applied
2nd	repeatable	procedures exist; they are not fully documented and do not cover all relevant aspects
3rd	defined	procedures are fully documented and implemented, and cover all relevant aspects.
4th	managed	reviews are conducted to assess the effectiveness of the controls in place
5th	optimized	regular review supports continuous improvement towards optimization of the given process

Table 1: Maturity levels of AICPA PMM

Model 2. - MITRE Privacy Maturity Model (MITRE PMM): this model is based on concepts in foundational laws and guidance applicable to U.S. organisations. The main pillars of the framework are the seven privacy elements of a privacy program. [23]

Level	Level name	Description
1st	ad hoc	privacy program requirements are not yet reliably implemented, or documented
2nd	defined	program requirements are documented but may not be implemented consistently
3rd	consistently implemented	program requirements are established and enforced standard business practices
4th	managed & measurable	requirements are managed along agreed metrics; process effectiveness is monitored
5th	optimized	continuous process improvement and automated monitoring of effectiveness

Table 2: Maturity levels of MITRE PMM

Model 3. - Minnesota Privacy Consultants Maturity Model (MPCMM): this model applies the methodology of AICPA PMM and extends it with an additional maturity level. MPCMM is special among the models because it is based on a risk-based approach measuring the risk of a privacy breach, regulatory noncompliance, or customer attrition. [16]

Level	Level name	Description
0	nonexistent	very high risk across the organisation
1st	initial	high risk across the organisation, and very high in key parts
2nd	repeatable	moderate risk across the organisation, with some pockets of high risk
3rd	defined	moderate risk across the organisation
4th	managed	low risk across the organisation
5th	optimized	risks are remote across the organisation

Table 3: Maturity levels of MPCMM

Model 4. - Security & Privacy Capability Maturity Model (SPCMM): this model aims to provide objective criteria for the assessment of cybersecurity and privacy controls. The model follows the structure of the Systems Security Engineering Capability Maturity Model[9]. [20]

Level	Level name	Description
0	not performed	controls are not performed
1st	performed informally	controls are performed, but lacks completeness & consistency
2nd	planned & tracked	practices are tailored to meet those specific requirements for controls
3rd	well-defined	practices are well-defined and standardised across the organisation
4th	quantitatively controlled	well-defined and standardised practices; detailed metrics to enable oversight
5th	continuously improving	well-defined, standardised practices; detailed metrics; continuous improvement

Table 4: Maturity levels of SPCMM

Model 5. - Privacy Road Web: this model is a focus area model enabling maturity assessment alongside seven focus areas having two to four levels. Being a focus area model the Privacy Road Web has no generic levels. The model integrates the activities an organisation needs to adopt in order

[9] Systems Security Engineering Capability Maturity Model (SSE-CMM) Project, Web: https://apps.dtic.mil/dtic/tr/fulltext/u2/a393329.pdf, (1999)

to be privacy respecting. [14]

Model 6. - ISACA Paris Chapter Maturity Model (ISACA MM): this model was developed as a multisectoral tool for enterprises to assess their maturity level of control as the requirements of privacy legislation concerns.. The model was publishes in French, the original level names are shown in brackets in *Table 5*. [12]

Level	Level name	Description
1st	incomplete (incomplet)	obligations are not fulfilled causing a complete lack of compliance.
2nd	partially compliant (conformité partielle)	obligations are met partially
3rd	optimized and compliant (optimisé et conforme)	organisation is deemed to be compliant with the legal requirements
4th	sustainable (pérenne)	compliance is sustainable, processes and their compliance are revised periodically
5th	leader (leader)	organisations at this stage go beyond the legal requirements

Table 5: Maturity levels of ISACA MM

Model 7. - Privacy Culture GDPR Maturity Framework (PCMF): Privacy Culture developed a nine-stage GDPR maturity framework where controllers need to fill a questionnaire on twelve privacy domains. The model provides an overall maturity score for each domain which enables organisations to assess their procedures and controls. [8]

Level	Level name	Description	Level	Level name	Description
0	non existent	score 0	5th	defined controls and fully implemented	scores 2.5-3
1st	initial but ad hoc	scores 0.5-1	6th	Managed controls but not benchmarked	scores 3-3.5
2nd	ad hoc but some controls	scores 1-1.5	7th	Managed controls and benchmarked	scores 4-4.5
3rd	repeatable controls	scores 1.5-2	8th	Optimal and independently verified	scores 4.5-5
4th	defined but not fully rolled-out	scores 2-2.5			

Table 6: Maturity levels of PCMF

Model 8. - Intel Privacy Maturity Model (Intel PMM): Intel developed a five-stage maturity model based on GAPP as well as AICPA/CICA Privacy Maturity Models and other industry criteria. The model applies the structure of the AICPA PMM but defines different privacy domains. [11]

Model 9. - Fort Privacy Maturity Model Framework (Fort PMMF): Fort Privacy developed a five-stage maturity model in order to bring much structure to data protection programs and provide a tool to measure their effectiveness. [8]

Level	Level name	Description
1st	ad hoc	chaos reigns at level 1 in an "ad hoc" ill-defined and undocumented world
2nd	established	the organisation has, at the very least, documented the requisite procedures
3rd	implemented	the organisation has implemented and adopted the documented procedures
4th	measured	quantitative measurement of the effectiveness of the adopted procedures
5th	optimised	procedures are constantly being improved after reviewing the feedback and measurements being reported

Table 7: Maturity levels of Fort PMMF

Model 10. - Personal Data Protection Maturity Model (PDPMM): this model offers a methodology for companies in the micro financial sector to improve their data protection capabilities. [9]

Level	Level name	Description
1st	none	organisations are totally or partially unaware of personal data protection
2nd	initial	organisations know data protection aspects starting to establish initial privacy processes
3rd	defined	organisations have defined processes related to data protection
4th	managed	processes are managed in a way that identification, analysis, and evaluation activities exist
5th	optimized	level of excellence; periodical process evaluation; high level of effectiveness

Table 8: Maturity levels of Fort PDPMM

Model 11. - Privacy Capability Maturity Model (PCMM): PCMM was developed for controllers in the telecommunication sector to assess organisational capabilities to protect information privacy. [19]

Level	Level name	Description
0	non existent	no data protection activities are performed in the organisation
1st	initial	ad hoc activities; no defined policies, or procedures; lack of teamwork and commitment.
2nd	repeatable	defined privacy policy; general awareness and commitment; specific plans in high-risk areas
3rd	defined	privacy policy and risk assessment; priority setting and coordination to deploy effective controls
4th	managed	consistently effective privacy management, privacy considerations reflected in the organisation
5th	optimizing	continuous improvement of privacy policies; changes are systematically scrutinised for privacy impact; dedicated resources to achieve privacy objectives; measured quality goals

Table 9: Maturity levels of PCMM

Model 12. - Privacy Maturity Assessment Framework (PMAF): this model was developed by the New Zealand Government to help agencies meet core expectations of the government in privacy management. [17]

Level	*Level name*	*Description*
1st	ad hoc	unstructured approach; initiatives by individuals rather than processes
2nd	developing	overall approach is largely reactive with some documented guidelines; limited central oversight
3rd	defined	privacy policies, processes and practices are defined and comprehensive; holistic and proactive approach with widespread awareness of privacy management
4th	embedded	well-defined governance and oversight structures exist.
5th	optimised	clear culture of continual improvement; leader in privacy management

Table 10: Maturity levels of PMAF

5. Comparative analysis of maturity models

This section aims to compare the characteristics of the above models in order to map the scene of privacy models and identify contingent needs to develop a new model. The following subsections analyse the models according to their methodological elements and general features.

5.1. Level names and number of levels

Analysing the structure of the models, most of them have five to six stages but the PCMF is an exceptional one providing a refined methodology to score privacy maturity at nine levels. If a model incorporates a “Level 0”, it symbolises the lack of the desired activities. In the rest of the models, “Level 1” may stand for the absence or the initial state of activities. Most of the models tend to use similar stage names to CMMI (initial, managed, defined, quantitatively managed, optimizing) [21] in case of upper levels. It can be assumed that these methodologies mainly follow the pattern of the CMMI model in terms of number of levels and the stage names.

Model	Level 0	Level 1	Level 2	Level 3	Level 4	Level 5
AICPA PMM		ad hoc	repeatable	defined	managed	optimized
Mitre PMM		ad hoc	defined	consistently implemented	managed & measurable	optimized
MPCMM	non-existent	initial	repeatable	defined	managed	optimized
SPCMM	not performed	performed informally	planned & tracked	well-defined	quantitatively controlled	continuously improving
Privacy Road Web	four stages without common stage names					
ISACA MM		incomplete	partially compliant	optimized & compliant	sustainable	leader
PCMF[10]	non existent	initial but ad hoc	ad hoc but some controls	repeatable controls	defined but not fully rolled-out	defined controls, fully implemented
Intel PMM		ad hoc	repeatable	defined	managed	optimized
Fort PMM		ad hoc	established	implemented	measured	optimised
PD PMM		none	initial	defined	managed	optimized
PCMM	non existent	initial	repeatable	defined	managed	optimizing
PMAF		ad hoc	developing	defined	embedded	optimised

Table 11: Comparison of model level names

5.2. Year, sector, country and source

This subsection compares the models based on their year of publication, targeted sector, country of origin and source. This comparison helps identifying the models that respond to the specific challenges of GDPR and the ones that foster the improvement of general privacy measures. Models are listed according to their year of publication.

Model	Year	Sector	Country	Source
PCMM	2007	Telecommunication	South Africa	scientific
AICPA PMM	2011	Business sector	Canada	non-scientific
MPCMM	2012	Commerce	USA	non-scientific
PMAF	2015	Government sector	New Zealand	non-scientific
Privacy Road Web	2015	Non-sectoral	Netherlands	scientific
ISACA MM	2017	Enterprises	France	non-scientific
PDPMM	2018	Microfinance	Peru	scientific
Fort PMM	2019	Non-sectoral	Ireland	non-scientific
Mitre PMM	2019	Non-sectoral	USA	non-scientific
PCMF	2019	Non-sectoral	UK	non-scientific
SPCMM	2019	Non-sectoral	USA	non-scientific
Intel PMM	N/A	Computer industry	USA	non-scientific

Table 12: comparison of general model features

Half of the models were published before the adoption of GDPR, between 2007 and 2015. The rest of the models were created after the adoption of the regulation. It can be conceivably hypothesised that GDPR gave a special impetus to the issue of privacy management globally.

The majority of the models published after the release of the GDPR is not sector-specific generally targeting a wider audience. These models are also applicable in the public sector providing state-of-the-art methodological assistance for the assessment of privacy programs.

According to their geographical origin, the examined models stem from different continents showing that privacy maturity measurement is a globally-accepted tool to improve privacy programs and

[10] This model has three more levels.

measures. It can be noted that the minority of the models were published in scientific journals. Taking into consideration the indisputable advantages of maturity models there is room for further research on this field.

5.3. Model domains and GDPR requirements

The number of domains varies model by model according to the pertinent regulatory framework or the objectives of the model. In many cases models use unique names but cover very similar process areas. This paper compares the above models by classifying model domains into common categories according to the main chapters of the GDPR prescribing obligations for data controllers and processors (Chapter II., III, IV., V. shown as Category 1-4 in *Table 13*).

Categories	**Classification**	**AICPA PMM**	**Fort PMM**	**Privacy Road**	**Intel PMM**	**Mitre PMM**	**PCMF**	**SPCMM**	**MPCMM**	**ISACA MM**	**PDPMM**	**PCMM**	**PMAF**
1. Principles (GDPR Chapter II.)	Transparency	x	x	x	x	x	x		x	x	x	x	
	Lawfulness	x	x			x	x		x	x		x	
	Accountability		x			x	x			x		x	x
	Further principles (purpose limitation, storage limitation, accuracy, data minimisation)	x	x		x	x	x		x	x	x	x	x
2. Data subject rights (GDPR Chapter III.)	Data subject rights	x	x	x	x		x		x	x		x	
3. Controller and processor (GDPR Chapter IV.)	Governance (General obligations, technical and organisational measures)	x	x	x	x	x	x	x	x	x	x	x	x
	Privacy by design			x	x	x	x			x		x	
	Data breach management		x		x	x	x		x	x		x	x
	Risk management		x	x		x	x	x	x	x	x	x	x
	Impact assessment			x			x			x	x		x
	Security	x	x		x	x	x		x	x	x	x	
	Training, awareness (Data protection officer)			x	x	x	x			x	x	x	x
	Third party management (third parties or data processors)	x	x		x	x	x		x	x		x	x
4. Transfers of personal data to third countries or international organisations (GDPR Chapter V.)	Trans border data flow (General principle for transfers)				x					x			

Table 13: Comparison of general model features

This article does not analyse whether the models are completely in line with the GDPR which could be the subject of a further more extensive research. As to the method of classification, domain descriptions and the related attributes were analysed in each model and domains were linked to the relevant articles or sections of the GDPR. *Table 13* shows which GDPR provisions are reflected in the models. In certain cases domains were linked to more than one category. The *appendix* illustrates the classification of model domains. [11]

Most of the models (*PCMM, AICPA PMM, MPCMM, PMAF, PDPMM, MITRE PMM, Intel PMM*) are targeted at compliance with non-European legislation or general privacy principles instead of GDPR compliance. Though the Privacy Road Web is European, it focuses on requirements of the pre-GDPR legislation. One of the models does not focus on organisational compliance rather than on cybersecurity and privacy controls (*SPCMM*). It can be assumed that models created after the release of the GDPR (*PCMF, ISACA MM, Mitre PMM)* respond to most requirements of the regulation.

GDPR views processing activities through the spectacles of risk. The “risk-based approach” goes beyond the “harm-based approach” taking into account every potential and actual adverse effect instead of concentrating only on damage. [6]. This is a holistic requirement determining the complete privacy management of an organisation. It can be noted that risk assessment is an integral element in almost all models. Nonetheless, risk is one of the model domains but not a holistic requirement in many cases. From this perspective, the MPC maturity model is an exceptional best practice where risk is the main determinant of maturity levels. This model, however, is based on U.S. privacy requirements. The SP-CMM model addresses some holistic risk considerations by stating that the risk associated with the controls in question decreases with maturity, however, it provides no further details.

Based on the findings above, it is advisable to develop a GDPR-specific model that addresses the relevant requirements of the regulation to achieve compliance and levels should be defined according to the risks taken. The methodology of the model shall take into account that the identified risks are not simple organisational ones but risks affecting the rights and freedoms of natural persons and maybe larger groups of people. Needless to say that controllers obligations are scalable according to the level of risks but data subject rights shall be respected regardless of the levels identified. [6]. Several experts believe that it is inevitable to regard risk as a holistic approach to privacy compliance not just because of the general risk-based approach of GDPR but also because it can be reasonably assumed that the desired or achieved privacy maturity level basically depends on the organisational risk appetite[12]. Risk appetite is dependent upon the business objectives of the organisation determining the scope of risks to be taken. [10, p7]

The different levels of privacy maturity may be defined by the appropriateness of the implemented measures indicating how much they are suited to reduce the risks of infringing the rights and freedoms of data subjects. [22, p.6.] The level of maturity shall be connected to the level of risks potentially threatening the rights and freedoms of data subjects because one of the main goals of GDPR is to eliminate or reduce the risks of data processing activities. Furthermore privacy risk can induce further business-related or organisational risks such as the financial consequences of non-compliance or a data breach. Decision makers might focus on the latter risk types and prioritize privacy risks to the

[11] It needs to be noted that certain models (Fort PMM, Intel PMM, PCMF) were available only in a summarized form for the public, so the comparison shown by Table 13 is made on the basis of the available information.

[12] The amount of risk that an organisation is prepared to accept, tolerate, or be exposed to at any point in time. The Orange Book: Management of Risk – Principles and Concepts HM Treasury, (2004)

extent they influence the running the business or the organization. The models examined use a different focus and do not evaluate the connection and the correlation of the different risk types. The planned new privacy maturity model shall address these linkages and support decision makers deciding which measures to take on the road to privacy compliance. The structure of the above models addressing most provisions of the GDPR and the risk based methodology of the MPC model can be used as a starting point for the new model.

Risks may appear in both public and private sectors. Hence, the new model shall be applicable in different sectors, in the course of the development of new products or services or the development of e-government solutions.

6. Summary and conclusions

In order to ensure a consistent level of protection for natural persons throughout the Union and to prevent divergences hampering the free movement of personal data within the internal market, the European Commission drew up a new data protection regulation (GDPR). Pursuant to this legislation controllers shall implement appropriate technical and organisational measures to ensure compliance. Besides, GDPR applies a risk-based approach to data processing activities, namely controllers shall comply with legal obligations according to the level of risks. [6] According to this paper, privacy compliance and the completeness of privacy programs could be best described with the methodology of maturity models. Based on the analysis of the pertinent literature, only a few researchers have nevertheless addressed the problem of privacy maturity.

This paper analysed twelve models available in the scientific discourse and in the business sector. These models stem from different continents showing that privacy maturity measurement is a globally accepted tool to improve privacy programs and measures. Model objectives are determined by the local regulatory environment or general privacy principles. It can be assumed that models created after the release of the GDPR respond to most requirements of regulation. As to the risk-based approach, it can be noted that risk assessment is an integral element of almost all models. Nonetheless, risk is one of the model domains but not a holistic requirement in many cases.

Based on the findings, it is advisable to elaborate a GDPR-specific model that addresses the relevant requirements to achieve compliance and its levels should be defined according to the risks taken. The planned new privacy maturity model shall handle the interconnections between different risk types and support decision makers deciding which measures to take on the road to privacy compliance. The elaboration of this model paves the way for further research and could provide a specific tool for organisations to measure their privacy management activities.

7. References

[1] AMERICAN INSTITUTE OF CERTIFIED PUBLIC ACCOUNTANTS, CANADIAN INSTITUTE OF CHARTERED ACCOUNTANTS: AICPA/CICA Privacy Maturity Model, Web: https://iapp.org/resources/article/2012-06-01-aicpa-cica-privacy-maturity-model/, 2011

[2] BECKER, J., KNACKSTEDT, R. and PÖPPELBUSS, P., Developing Maturity Models for IT Management - A Procedure Model and its Application. Business & Information Systems Engineering 1(3), pp. 213-222, (2009)

[3] BEKKERS, W., VAN STEENBERGEN, M., BOS, R., BRINKKEMPER, S., and VAN DE

WEERD, I., The design of focus area maturity models. In: Winter, R., Zhao, J.L., Aier, S. (eds.) DESRIST 2010. LNCS, vol. 6105, pp. 317–332. Springer, Heidelberg, (2010)

[4] BRUIN, T. DE, FREEZE, R., KULKARNI, U. and ROSEMANN, M., Understanding the Main Phases of Developing a Maturity Assessment Model. In: Proceedings of the 16th Australasian Conference on Information Systems. Sydney, (2005)

[5] CARALLI, R. A., KNIGHT, M. and MONTGOMERY, A., Maturity Models 101: A Primer for Applying Maturity Models to Smart Grid Security, Resilience, and Interoperability, Carnegie Mellon University, Software Engineering Institute, Pittsburgh, (2012)

[6] EUROPEAN COMMISSION - ARTICLE 29 DATA PROTECTION WORKING PARTY: Statement on the role of a risk-based approach in data protection legal frameworks, Web: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm, (2014)

[7] EUROPEAN PARLIAMENT AND OF THE COUNCIL: Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Official Journal, Bruxelles, (2016)

[8] FORT PRIVACY: Introducing the privacy maturity model framework, Web: https://www.fortprivacy.ie/privacy-maturity-model/, (2019)

[9] GARCIA, A., CALLE, L., RAYMUNDO, C., DOMINGUEZ, F. and MOGUERZA, J. M., Personal Data Protection Maturity Model for the Micro Financial Sector in Peru, 4th International Conference on Computer and Technology Applications, IEEE, (2018)

[10] HM TREASURY: Thinking about risk, Managing your risk appetite: A practitioners guide, HM Treasury, London, (2006)

[11] INTEL: Overview of Privacy Maturity Model, Web: https://iapp.org/media/presentations/13Academy/A13_ Caring_For_Acquistions_HO5.pdf

[12] ISACA PARIS CHAPTER: Modéle de maturité, Web: http://imedia-conseil-dev.fr/AFAI/guide-donnees-personnelles-Afai-2017.pdf, (2017)

[13] LAHRMANN, G., MARX, F., METTLER, T., WINTER, R. and WORTMANN, F., "Inductive Design of Maturity Models: Applying the Rasch Algorithm for Design Science Research". Service-Oriented Perspectives in Design Science Research. Springer. pp. 176–191, (2010)

[14] LIESHOUT, M. and HOEPMAN, J. H., The PI.lab - Four years later, The Privacy & Identity Lab, Nijmegen, (2015)

[15] METTLER, T., "Maturity assessment models: a design science research approach". International Journal of Society Systems Science. 3 (1/2): 213–222., (2011)

[16] MINNESOTA PRIVACY CONSULTANTS: MPC Privacy Maturity Model for consumer data, Web: https://iapp.org/media/pdf/knowledge_center/MPC_Privacy_Maturity_Model_for_

Consumer_Data_2012.xlsx, (2012)

[17] NEW ZEALAND GOVERNMENT: Using the Privacy Maturity Assessment Framework, Web: https://snapshot.ict.govt.nz/resources/digital-ict-archive/, (2015)

[18] PRIVACY CULTURE LTD.: The GDPR maturity framework, Web: https://www.privacyculture.com, (2019)

[19] REDDY, K. and VENTER, H. S., Privacy Capability Maturity Models within Telecommunications Organisations, University of Pretoria, SATNAC 2007 Conference Papers, (2007)

[20] SECURE CONTROLS FRAMEWORK: Security & Privacy Capability Maturity Model, Web: https://www.securecontrolsframework.com/sp-cmm, (2019)

[21] SOFTWARE ENGINEERING INSTITUTE: CMMI for Development, (Version 1.3), Carnegie Mellon University Software Engineering Institute, (2010)

[22] THE EUROPEAN DATA PROTECTION BOARD: Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, (2019)

[23] THE MITRE CORPORATION: Privacy Maturity Model, Web: https://www.mitre.org/publications, (2019)