Table 1: Context of Employment of DPOs - Questions

QN	Question	Answer options
1.1	Does your company belong to the public or private sector?	Private, Public
1.2	What is the activity sector of your company?	followed the classification of the ISIC[a]

a International Standard Industrial Classification of All Economic Activities (ISIC) is an international reference classification of productive activities. These activities are classified according to the type of economic activity they engage in.

Table 2: Characterization and background of DPOs - Questions

QN	Question	Answer options
2.1	What is your age?	Numeric selector
2.2	What is your gender?	Female, Male
2.3	What are your educational qualifications?	followed the classification of the ISCED[a]
2.4	What is the field of your education?	followed the classification of the ISCED-F[b]
2.5	Do you have any training related to the GDPR or the DPO role?	Yes, No

a International Standard Classification of Education (ISCED) is a referential, created for compiling and presenting education statistics. In the current context, it was used the revision ISCED 2011.

b ISCED-F 2013 is a referential focused on the fields of education and training.

Table 3: Contractual relationship of DPOs - Questions

QN	Question	Answer options
3.1	Are you an internal DPO or externally contracted?	Internal employee, External (Outsourcing)
3.2	Do you accumulate the position of DPO with other activities in the organization?	Yes, No
3.3	In case you are an internal DPO, have you had your income reviewed when assuming the DPO role?	Yes, No

Table 4: Contractual relationship of DPOs - Questions

QN	Question	Answer options
4.1	Was the decision to be a DPO compelled or unforced?	Compelled Decision, Unforced Decision
4.2	How satisfied are you with the role?	Very unsatisfied, Not satisfied, Neutral, Satisfied, Very satisfied

4.3	Are you willing to proceed with the DPO role or quit this role?	Proceed, Quit

Table 5: ISIC classification of economic activities - Answers

ISIC Section	Number	%
Section O - 8411 General public administration activities	30	19.48%
Section Q - Human health and social work activities	22	14.29%
Section P - Education	16	10.39%
Section O - 8423 - Public order and safety activities	11	7.14%
Section J - Information and communication	11	7.14%
Section K - Financial and insurance activities	10	6.49%
Section H - Transportation and storage	10	6.49%
Section C - Manufacturing	8	5.19%
Section S - Other service activities	6	3.90%
Section M - Professional, scientific, and technical activities	6	3.90%
Section I - Accommodation and food service activities	6	3.90%
Section D - Electricity, gas, steam, and air conditioning supply	5	3.25%
Section N - Administrative and support service activities	3	1.95%
Section G - Wholesale and retail trade	3	1.95%
Section A - Agriculture, forestry, and fishing	1	0.65%
Section O - 8422 Defence activities	1	0.65%
Multiple areas defined	5	3.25%
Total	154	100%

Table 6: Answers to QN2.1 related to the age of DPOs

Responses for QN2.1 (age)	Number	%
Less than 30	12	7.8%
From 31 to 40	34	22.1%
From 41 to 50	57	37.0%

Higher than 50	41	26.6%
No answer	10	6.5%
Total	154	100%

Table 7: ISCED 2011 qualification - Answers

ISCED 2011 level	Qualification	Number	%
Level 8	Doctoral	6	3.9%
Level 7	Master's	55	35.7%
Level 6	Bachelor's	89	57.8%
Level 5 or Lower	Secondary	4	2.6%
Total		154	100%

Table 8: ISCED-F 2013 Fields of Education - Answers

ISCED-F 2013 Field	Number	%
042 - Law	61	39.4%
061 - Information and Communication Technologies	44	28.4%
041 - Business and administration	28	18.1%
031 - Social and behavioural sciences	6	3.9%
Others	16	10.3%
Total	154	100%

Table 9: Responses for QN3.3 related to the income change (internal DPOs)

Responses for QN3.3 (income)	Number	%
No (the income was not revised)	100	80.7%
Yes (the income was revised)	19	15.3%
No answer	5	4.0%
Total	124	100%

Table 10: Responses for QN4.2 related to the level of satisfaction with the DPO role

Responses for QN4.2	Number	%
Very Satisfied	18	11.7%
Satisfied	74	48.1%
Neutral	42	27.3%
Unsatisfied	8	5.2%
Very Unsatisfied	12	7.8%
Total	124	100%

Practitioner's Corner

Managing Data Protection Compliance through Maturity Models: A Primer

*Friederike Knoke and Iheanyi Nwankwo**

I. Introduction

The quest to comply with the GDPR since its adoption in 2016 has given rise to several models suggesting how to comply with the various requirements of the regulation. These models focus on different aspects of data protection; for example, the Standard Data Protection Model (SDM)[1] focuses on implementing technical and organisational measures, while the Privacy Risk Analysis Methodology PRIAM[2] is a privacy risk assessment model. A slightly different way of approaching compliance is using a maturity model. A maturity model is a model to describe and evaluate how an entity makes progress in achieving a specific target. Such a model, applied in the field of data protection, comes along with analysing the requirements to fulfil GDPR rules in a qualitative, development-oriented way to improve the data protection performance continuously. It could be seen as an indicator matrix to quickly identify compliance requirements and maturity levels. Therefore, this concept offers an opportunity for self-evaluation as it can identify a gap and suggests steps to improve the capability level.

Over the years, several fields have adopted maturity assessment models to ascertain and measure specific aspects of maturity, ranging from people to process and systems maturity.[3] In data protection, such models offer a reliable indicator to measure an organisation's data protection compliance posture. When properly utilised, it not only presents an opportunity to improve the compliance capability of an entity but also provides an avenue for data subjects and other actors involved in the data processing chain to evaluate and eventually trust the process. With a consistent, quantifiable and comparable set of maturity indicators, there is a potential for an organisation to achieve significantly high levels of performance concerning its handling of personal data.

Recently, some attention has been drawn to the use of a maturity model in data protection following the publication of the French data protection authority Commission Nationale de l'Informatique et des Libertés (CNIL)'s Data Protection Management Maturity Self-Assessment model, which quantifies the rigour and formalism of activities related to data protection management by organisations.[4] Organisations can utilise it as a self-assessment model. While

DOI: 10.21552/edpl/2022/4/14

* Friederike Knoke and Iheanyi Nwankwo are research associates at the Institute for Legal Informatics, Leibniz University Hannover; this report is based on their work for the project 'Smart Dispatcher for Secure and Controlled Sharing of Distributed Personal and Industrial Data' (smashHit). The work in smashHit is funded by the European Commission under European Union's Horizon 2020 research and innovation programme, under grant agreement No. 871477. For correspondence <friederike.knoke@iri.uni-hannover.de> and <nwankwo@iri.uni-hannover.de>.

1 AK Technik of the Independent Data Protection Supervisory Authorities of the Federation and the Länder, 'The Standard Data Protection Model. A method for data protection advising and controlling on the basis of uniform protection goals', Version 2.0b (English version), April 2020 <https://www.datenschutzzentrum.de/uploads/sdm/SDM-Methodology_V2.0b.pdf> accessed 7 December 2022.

2 Sourya Joyee De, Daniel Le Métayer, 'PRIAM: A Privacy Risk Analysis Methodology', [Research Report] RR-8876 (2016) <https://hal.inria.fr/hal-01302541/document> accessed 7 December 2022.

3 See Michael Kohlegger, Ronald Maier, and Stefan Thalmann, 'Understanding maturity models. Results of a Structured Content Analysis' (2009) <https://www.researchgate.net/publication/215312013_Understanding_Maturity_Models_Results_of_a_Structured_Content_Analysis> accessed 7 December 2022, 1 ff.

4 CNIL, 'Autoévaluation de maturité en gestion de la protection des données. Un modèle pour se positionner et choisir les actions à mener' (2021) <https://www.cnil.fr/sites/default/files/atoms/files/autoevaluation_de_maturite_en_gestion_de_la_protection_des_donnees.pdf> accessed 7 December 2022.

this is a positive development in the EU data protection framework, there is yet no significant analytical discussion on the conceptual framework of maturity models in data protection. There is still no detailed analysis of how they could be applied to several aspects of data protection regimes, from software development to organisational implementation of data protection obligations.

As a deeper understanding of maturity model is necessary for its effective application in the area of data protection, the primary goal of this report is to give an overview of the concept and show its applicability in the field with the help of an example from a research project. The report presents the results of an in-depth analysis of a maturity model that seeks to implement data protection by design in the context of software development. The output, it is hoped, will inform the future development of maturity models in the various data protection domains.

To this end, the following is structured as follows: first, the concept of a maturity model and its definition is examined, followed by an overview of its development in the privacy and data protection field. Finally, the execution of a data protection maturity model is exemplified before the conclusions.

As a starting point it is necessary to understand that a data protection maturity model is a broad concept; nevertheless, it can be narrowed down and specifically applied to several areas of the data protection circle depending on the organisational needs and environment. Therefore, this report's ultimate goal is to open a broader discussion around maturity models with a potential for harmonisation in the future. In identifying relevant documents discussing maturity models a focus was put on works containing a) data protection maturity models, b) privacy maturity models, c) maturity metrics, and d), preferably, were published after the GDPR's adoption.

II. Conceptualising the 'Maturity Model' and its Application in Data Protection

1. Conception and Definition

The concept of a maturity model evolved as a valuable instrument to assist in evaluating an entity's progress over time as well as identifying reasonable improvement measures to meet a desired state.[5] Several attempts have been made at formally conceptualising and defining this concept. However, there is no consensus on this front, mainly because maturity models are meant to apply in different contexts, sometimes unrelated. Kohlegger, Maier and Thalmann analysed 16 models, and the result motivated them to define a maturity model as a conceptual representation of 'phases of increasing quantitative or qualitative capability changes of a maturing element in order to assess its advances with respect to defined focus areas'[6]. For them, the maturing element could be a person, object or social system, while focus areas include the maturity of processes, digital resources or people's competencies. Some 'trigger' conditions mark each phase of the maturity sequence, which a maturing element must fulfil before it can be assigned to the relevant stage. They further note that maturity models can be used descriptively to explain changes in reality, or normatively to guide managers to make interventions for more effective or efficient changes in the maturity element.[7]

The industry standard ISO/IEC 33001:2015[8] sees a maturity model in the light of being an assessment framework that defines a set of categories to be used to assess the capability of an entity to reach the desired goal. It defines it as a 'model derived from one or more specified process assessment model(s) that identifies the process sets associated with the levels in a specified scale of organizational process maturity'[9]. Here, the assessment is carried out by assigning each category's maturity or capability level. Each level is defined, and the processes associated with each level in a specified scale of organisational process maturity are identified.[10] 'Process maturity' in that context refers to the extent to which a specific process

5 Roberto Santana Tapia and others, 'Towards a business-IT alignment maturity model for collaborative networked organizations' (2008), 2008 12th Enterprise Distributed Object Computing Conference Workshops, 276. See also Jörg Becker, Ralf Knackstedt, and Jens Pöppelbuß, 'Developing Maturity Models for IT Management' (2009), Business and Information System Engineering No. 3, 213.

6 Michael Kohlegger, Ronald Maier, and Stefan Thalmann, 'Understanding maturity models. Results of a Structured Content Analysis' (2009), 10 <https://www.researchgate.net/publication/215312013_Understanding_Maturity_Models_Results_of_a_Structured_Content_Analysis> accessed 7 December 2022.

7 Ibid, 10.

8 ISO/IEC 33001:2015 Information technology - Process assessment - Concepts and terminology <https://www.iso.org/standard/54175.html> accessed 12 January 2023.

9 Ibid, 3.3.7 <https://www.iso.org/standard/54175.html> accessed 12 January 2023.

10 Ibid.

is explicitly defined and managed and how it is effectively measured and controlled.[11]

From the definitions above, it could be said that the concept of a maturity model is understood broadly, allowing it to play several roles in practical terms. When viewed independently, the word 'maturity' implies evolutionary progress to demonstrate an ability to accomplish a target from an initial to desired end stage.[12] At the same time, a 'model' on its part 'represents a formal description of (...) some aspects of the physical or social world around us for the purposes of understanding and communication'[13]. Thus, maturity models can be used in different areas of industry to support monitoring and improving the performance of a business. For example, the 'SANS Security Awareness Maturity Model'[14] is a model for managing and measuring an organisation's security awareness level. It focuses on 'an organisation's ability to effectively identify, manage, and measure its human risk'. It is a model to enable organisations 'to identify and benchmark the current maturity level of their security awareness program and determine a path to improvement'[15]. Its five maturity levels are defined as follows:

- **Non-existent**: No security awareness program is in place and employees can easily become victims of security attacks.
- **Compliance-focused**: The security awareness program is designed for compliance or audit purposes; employees are trained annually, or ad hoc and have little understanding of their role; there are security awareness professionals, but they act disconnectedly.
- **Promoting Awareness & Behavioural Change**: The security awareness staff is integrated into the security team and continuously communicates security topics internally; training takes place regularly (more often than once a year), and there is knowledge about security policies among the employees, which actively support the security goals.
- **Long-term Sustainment & Culture Change**: There are sufficient processes, resources and leadership support to make the security program an established part of the organisational culture; a program review and update is carried out at least annually.
- **Metrics Framework**: A robust metrics framework is in place to track and measure the impact of the program, the program is continuously improving and able to demonstrate return on investment.[16]

These maturity levels help assess the current situation in the organisation and the result can serve as a basis for internal actions. At the same time, the maturity levels can serve as a 'blueprint' for the stages to be achieved. This illustrates that maturity models can be deployed as a diagnostic tool[17], allow the identification of desirable target levels of maturity and guiding measures to reach increased maturity. These are beneficial for organisational improvements.[18] In the SANS maturity model, the training of employees, professional staff managing the topic, leadership support and integration of the program in the organisational 'culture' are crucial aspects for improvement.[19] In sum, the SANS maturity model mainly addresses *organisational* aspects related to security awareness in an organisation/company.

In contrast, some other maturity models suggest a rather *process-oriented* assessment. An example is the SPICE (Software Process Improvement and Capability Determination) model[20], which evolved from the CMM model[21], and was initially established for the assessment of the software supplied to the US

11 Tobias Mettler, 'Maturity assessment models: a design science research approach' (2011), Int. J. Society Systems Science, Vol. 3, Nos. 1/2, 81 (83). This author identified three focus areas of maturity models: process maturity, object maturity and people's capability.

12 Ibid, 81 (83).

13 Ibid, 81 (86), citing J. Mylopoulos, 'Conceptual modelling and telos', in P. Loucopoulos and R. Zicari (eds.), *Conceptual Modelling, Databases and Case*, 49 (51), John Wiley and Sons, 1992).

14 SANS 2022 Security Awareness Report: Managing Human Risk (2022), 4 <https://go.sans.org/lp-wp-2022-sans-security-awareness-report> accessed 7 December 2022.

15 Ibid, 4 <https://go.sans.org/lp-wp-2022-sans-security-awareness-report> accessed 7 December 2022.

16 Ibid, 4 et seq.

17 Anja M. Maier, James Moultrie, and P. John Clarkson, 'Developing maturity grids for assessing organisational capabilities: Practitioner guidance', in *4th International Conference on Management Consulting, Academy of Management (MCD)* (2009).

18 J. Becker, R. Knackstedt, and J. Pöppelbuß, 'Developing Maturity Models for IT Management, Business & Information Systems Engineering' (2009), 1(3), 213.

19 SANS 2022 Security Awareness Report: Managing Human Risk, 2022, 8 et seq <https://go.sans.org/lp-wp-2022-sans-security-awareness-report> accessed 7 December 2022.

20 Alec Dorling, 'SPICE: Software Process Improvement and Capability dEtermination' (1993), Software Quality Journal, No. 2, 209.

21 Christiane Gresse von Wangenheim and others, 'Systematic Literature Review of Software Process Capability/Maturity Model', in *Proceedings of International Conference on Software Process. Improvement and Capability dEtermination (SPICE)* (2010).

Department of Defence.[22] Later, it evolved into an international ISO standard.[23] SPICE provides a model for assessing software development processes and all processes relating to the software life cycle, including project management, e-learning and quality assurance.[24] The Automotive SPICE or ASPICE model applies the SPICE model to the automotive industry for software process improvement and capability.[25] The five levels of the ASPICE model can be summarised as follows:

- **Level 1 – Performed**: All software development processes are fulfilled, along with proper documentation.
- **Level 2 – Managed**: This means that the entire development process is fully managed. It also proves that the supplier has trained programmers along with proven management processes in place.
- **Level 3 – Established**: Here, the processes defined during level 2 have been established over time. Therefore, the process will be constantly evaluated, and the outcomes will be studied for further improvement.
- **Level 4 – Predictable**: Along with establishing and meeting the required performance standards, outcomes are constantly measured, documented, and analysed to enable evaluation. The processes and outcomes are established so well that outcome prediction becomes possible and easy.
- **Level 5 – Innovating**: At the innovation level, the software developer understands and controls their processes very well and can push boundaries by continuously optimizing the process and making them better.

From the discussion above, the generic nature of maturity models and their flexibility allows them to be applied in several fields. The following section shall therefore focus on how maturity models are applied in data protection.

2. Maturity Models in the Field of Data Protection

As already alluded to, the notion of maturity model has been advanced in the field of privacy and data protection. The earliest evidence of introducing the concept into the privacy sphere was by the American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA). They published a 'Privacy Maturity Model' in 2011 to assess procedures or processes in place in an organisation to protect privacy.[26] This model incorporated five maturity levels:

1. **Ad hoc**: Procedures or processes are generally informal, incomplete, and inconsistently applied.
2. **Repeatable**: Procedures or processes exist; however, they are not fully documented and do not cover all relevant aspects.
3. **Defined**: Procedures and processes are fully documented and implemented, and cover all relevant aspects.
4. **Managed**: Reviews are conducted to assess the effectiveness of the controls in place.
5. **Optimised**: Regular review and feedback are used to ensure continuous improvement towards optimisation of the given process.[27]

Since the AICPA and CICA publication, only a few other works have been done in this area. In 2018, Cisco used the AICPA/CICA model within the Privacy Maturity Benchmark Study.[28] The study investigated delays in the sales cycle due to data privacy issues, e.g. because customers ask questions about details of personal data and how it is processed during the sales. The study involved a double-blind survey where participants were asked to self-assess the level of privacy maturity of their organisation's privacy processes. By analysing the achieved privacy maturity level along with the sales delays due to privacy concerns, the study identified a correlation between the expe-

22 Watts S. Humphrey, 'Characterizing the Software Process: A Maturity Framework', in *Technical Report of the Software Process Feasibility Project Software Engineering Institute*, CMU/SEI-87-TR-11 (1987).

23 First ISO/IEC 15504 for process assessment; in 2015, it evolved into ISO 33001 published under the ISO 330xx family of standards for process assessment.

24 For details see Christiane Gresse von Wangenheim and others, 'Systematic Literature Review of Software Process Capability/Maturity Model,' in *Proceedings of International Conference on Software Process. Improvement and Capability dEtermination (SPICE)* (2010).

25 S. Thomas, *Automotive SPICE: Determining Software Process Improvement and Capability* (2021).

26 American Institute of Certified Public Accountants and Canadian Institute of Chartered Accountants, 'AICPA/CICA Privacy Maturity Model' (2011) <https://vvena.nl/wp-content/uploads/2018/04/aicpa_cica_privacy_maturity_model.pdf> accessed 12 January 2023.

27 Ibid, 2 <https://vvena.nl/wp-content/uploads/2018/04/aicpa_cica_privacy_maturity_model.pdf> accessed 12 January 2023.

28 Cisco, Cisco 2018 Privacy Maturity Benchmark Study (2018), 1 <https://iapp.org/media/pdf/resource_center/Cisco-2018-privacy-maturity-benchmark-study.pdf> accessed 7 December 2022.

rienced sales delay and the organisation's reported level of privacy maturity. The higher the level of privacy maturity an organisation had, the lower the indicated duration of the observed sales delays due to privacy concerns.[29] That way, the use of maturity levels in this survey provided an avenue to quantify the importance and (financial) benefit of organisation's investments in privacy processes.

Recently, the CNIL published a Data Protection Management Maturity Self-Assessment model to quantify the rigour and formalism of activities related to data protection management by organisations.[30] The model recognises that data protection activities in organisations are not always harmonised, and attempts to develop standard and generic activities with a five-level maturity approach (with an additional zero level indicating non-existent or incomplete actions). Although these maturity activities intend to transpose the IT security industry standard ISO/IEC 21827[31] and the ANSSI's ISS Maturity Guide[32], they also considered the GDPR and French data protection law. The table below summarises the CNIL model.

Although the CNIL application of the concept of a maturity model is novel since the adoption of the GDPR, it does not include a clear conceptualisation and concrete definition of the concept. This is understandable because a maturity model's role in data protection is sometimes complex, challenging and multi-faceted. However, using this model in all possible data protection scenarios the developer intended may require further contextual adjustment in many cases. For example, the eight typical data protection activities used as examples to structure possible actions taken in organisations do not cover activities such as software development. Moreover, it will be challenging to have a data protection model that covers all data protection activities, given the diverse nature of data protection requirements and the regulatory environment. It is also notable that legal rules constitute specific *obligations* to the norm addressees and do not accommodate gradation in compliance. Therefore, it may be difficult to assess the actions required of an entity to comply with the law as having been more or less mature; instead, they need a yes/no assessment in either a) the legally prescribed action has been taken or b) the legally prescribed action has not been taken.

This must be considered when conceptualising and defining a data protection maturity model. Given these challenges, one way to conceptualise a data protection maturity model is as a way of measuring the progress of an organisation in implementing data protection requirements in specific situations. Such models can be designed so that management and others responsible for complying with data protection obligations can easily understand the requirements and possible ways of operationalising them in specific cases, thereby presenting them with a matrix of measures to attend the desired state. Thus, a data protection maturity model can be defined as:

> *A conceptual representation of the phases of incremental changes that occur in the capacity of a personal data processing framework in order to assess their advances against specific aspects of data protection requirements or compliance targets.*

This approach provides an intuitive way of capturing the often complex and multi-faceted data protection compliance requirements. In addition, it accommodates targeting maturity models to specific areas of data protection, ranging from software development to international data transfers. The following shall exemplify this approach within the context of implementing technical and organisational measures within a system development lifecycle.

III. Implementing a Maturity Model in Data Protection: an Example from the smashHit Project

Having defined a data protection maturity model in the previous section, this section illustrates how such a model could be applied to a particular target of compliance using the 'smashHit' project as an example. The smashHit project is a research project funded under the European Commission's framework programme Horizon 2020, where a platform for the man-

29 Ibid, 4.

30 CNIL, 'Autoévaluation de maturité en gestion de la protection des données. Un modèle pour se positionner et choisir les actions à mener' (2021), 1 ff. <https://www.cnil.fr/sites/default/files/atoms/files/autoevaluation_de_maturite_en_gestion_de_la_protection_des_donnees.pdf> accessed 7 December 2022.

31 ISO/IEC 21827:2008 Information technology — Security techniques — Systems Security Engineering — Capability Maturity Model.

32 <https://www.ssi.gouv.fr/uploads/2009/07/maturitessi-methode-2007-11-02.pdf> accessed 7 December 2022.

Table 1: CNIL Data Protection Management Maturity Self-Assessment model levels and features

Levels	Features
0 – Non-existent or incomplete practice	Nothing is done in terms of data protection. As a result, it is not known or supported within the organisation, and the need is not recognised.
1 – Informal practice (some isolated actions)	Actions are performed using Routine Practices. They are implemented informally and in response to isolated requests, without any real commitment from the managers of the organisation or real coordination between those who implement these actions.
2 – Repeatable and followed practice (reproducible actions)	The actions are carried out by a person who possesses data protection skills. Actions are planned. Some practices are formalised, which allows duplication and reuse (possibly by another person). The managers of the organisation monitor data protection, but the entire profession is far from being involved. Qualitative measurements are carried out (simple indicators of the result, e.g. consideration of data protection in this or that project).
3 – Defined process (standardisation of practices)	Actions are carried out in accordance with a defined process (e.g. use of methods), standardised (common to all in the organisation) and formalised (existence of documentation). The persons carrying out the actions have the skills appropriate to the process. The organisation supports the process (provides the resources, means and training necessary for its operation). The process is well understood by both management and the performers.
4 – Controlled process (qualitative measurement and defect correction)	The process is coordinated throughout the chosen scope and for each run. Quantitative measurements are regularly carried out (in performance terms, e.g. proportion of projects considering the data protection). The measurements taken (qualitative and quantitative indicators) are analysed (e.g. someone is in charge of studying the indicators and proposing an analysis and an action plan). Improvements are made to the process based on analysis of the measurements taken.
5 – Process continuously optimised (continuous improvement)	The process is dynamically adapted to the situation (improvements and changes are directly integrated). The analysis of the measurements taken is defined, standardised and formalised. Process improvement is defined, standardised and formalised. The evolution steps of the process are traced.

agement of consent and its metadata, e.g., in the car insurance and smart city environment, has been developed.[33] The development of the system follows the principles of data protection by design, which translates to, among others, implementing specific technical and organisational measures (TOMs) aimed at securing the system and mitigating the risks posed to subjects whose data will be processed by the system.

The role that the maturity model is called to play here is to measure the TOMs implementation capabilities during system development. Precisely, within the smashHit project, a maturity model was used for three purposes: 1) to describe current privacy-preserving procedures and technologies in place within the context of executing privacy by design, 2) to pre-

33 'smashHit' is an acronym for the project title 'Smart Dispatcher for Secure and Controlled Sharing of Distributed Personal and Industrial Data'. For more information about the project, see the project website: <https://www.smashHit.eu> accessed 12 January 2023.

scribe areas for improvement to be addressed in order to reach GDPR compliance, but also higher levels of privacy assurance, and 3) to provide an indication of different capabilities, which could serve as vital benchmarks for the data subjects when deciding on granting consent for data sharing.

The CNIL model played a significant role during the development of the smashHit maturity model because of its adaptable nature. The researchers in smashHit, therefore, adapted it to measure the implementation of technical and organisational measures for executing privacy by design. The following adaptions were made in the smashHit model: Firstly, it retained the five maturity levels from the CNIL model (excluding the zero level), but the criteria or benchmark for each level (known as 'features' in the CNIL model) were modified or interpreted to suit the software development lifecycle. Secondly, these criteria as well as the objects of the assessment, were defined contextually. For example, it was contemplated that different legal requirements and principles of data protection should be considered at the early stages of data processing activities before the actual processing begins. In the case of software development, this means from the beginning of the software development process, e.g. during the requirements analysis and design of the software architecture.[34] This is laid down in Article 25 GDPR, which obliges the controller to follow the principle of data protection by design already 'at the time of the determination of the means for processing'.

It is important to note that, like other legislation, the GDPR stipulates some obligations in abstract and normative statements instead of specifying concrete actions for norm addressees. Consequently, it is the responsibility of the system developers to transpose the legal requirements into concrete actions and activities. In this case, the SDM Model offered a method for selecting and evaluating TOMs that operationalise data protection principles by design. The SDM model identifies seven protection goals, which reflect and bundle the objectives of different requirements of the GDPR,[35] to suggest reference measures to achieve each protection goal[36]. However, as a whole, the SDM is not limited to these protection goals and the proposed reference measures; it goes further to suggest a procedure to evaluate and control data protection measures. This allowed the smashHit project to regard the TOMs as the implementation activities to execute the principle of privacy by design.

Since TOMs help to fulfil the protection goals, the level of implementation can be utilised to indicate to what extent a system development considers privacy protection goals. Therefore, the description of smashHit's maturity levels relates to the level of maturity of the implementation of the TOMs. On top of that, the protection goals and reference measures from the SDM form the objects of assessment. To allow a verifiable assessment of each measure with the help of capability dimensions, the wording of the CNIL reference measures was modified. This resulted in the development of the following maturity levels for smashHit:

1. **Performed**: The TOMs are implemented informally and in isolation.
2. **Managed**: The TOMs are planned by skilled persons and implemented in a managed fashion.
3. **Monitored**: The TOMs are implemented within a defined process and the implementation is monitored to assure they achieve the desired outcome.
4. **Controlled and coordinated**: The TOMs are implemented in a coordinated process including analysing measurements.
5. **Continually optimised**: The TOM implementation continually improves to respond to changes, based on a formalised and standardised process.

In this smashHit Maturity Model, level 1 is the lowest in the maturity capability, where implementation of TOMs in the system development is done informally and isolated. No one is responsible for ensuring that these measures are undertaken at the earliest point of the system development to comply with the principle of data protection by design. Level 2 shows that TOM implementation is managed by skilled persons and planned during the system development. At a higher level, Level 3, these planned activities are implemented within defined procedures and, above all, are monitored to ensure the desired outcome. At Level 4, apart from implementing and monitoring the TOMs, the outcome is analysed and measured. This is well coordinated so that feed-

34 Requirements analysis and design of the software architecture are phases in the Software Development Lifecycle (SDLC) see wikipedia <https://en.wikipedia.org/wiki/Software_development_process#Waterfall_development> accessed 7 December 2022.

35 SDM, 10 et seq.

36 SDM, 31 et seq.

back from the analysis is translated into the system development process of the organisation. Finally, Level 5 is at the highest level, where the implementation is continually improved to adapt to circumstances. At this stage, the process is formalised, and standard procedures exist for this.

In summary, the adoption of a maturity model-based approach for assessing the capability of the implementation of TOMs within the smashHit project involved the adaptation of three major elements:

- Adaptation of the maturity level definitions from existing maturity models to align with the assessment of software development
- Adaptation of the level and object definitions to align with the requirements for GDPR compliance; and
- Factoring the guidelines provided in each of the TOMs from the SDM into separate and individually verifiable measures for assessment.

IV. Conclusion

This analysis has shown that the concept of maturity models is characterised by the flexibility that allows applications in various fields. Concretely, their use offers a promising extension of management tools in the data protection and privacy field. Based on general conceptualisations of models for the assessment of maturity as well as existing applications to the field of data protection, we define a 'data protection maturity model' as *a conceptual representation of the phases of incremental changes that occur in the capacity of a personal data processing framework in order to assess their advances against specific aspects of data protection requirements or compliance targets*.

However, taking into account the specifics of the concrete context is of great importance when adapting a maturity model. Where the aim of the model is to provide information on compliance with legal requirements, e.g. laid down in the GDPR, attention needs to be paid to the model's conceptualisation to ensure the maturity model technique is compatible with evaluating a context with legal obligations. The example maturity model from the smashHit project illustrates how a maturity model can be adapted and implemented to measure the level of implementation of the data protection by design principle in software development.

Finally, the specifics of data protection rules affect the overall result of any model's assessment. This means that the conclusion of the assessment should either confirm compliance with GDPR rules or conclude that the GDPR requirements are not met. Therefore, further work is needed in standardising future models if aimed at capturing all possible scenarios.