Demonstration of the DPMF for Data Protection Analysis

Laurens Sion [*], Dimitri Van Landuyt [*], Pierre Dewitte [†], Peggy Valcke [†], Wouter Joosen [*]
[*] imec-DistriNet, KU Leuven
firstname.lastname@cs.kuleuven.be
[†] imec-CiTiP, KU Leuven
firstname.lastname@kuleuven.be

***Abstract*—Frameworks such as the EU General Data Protection Regulation (GDPR) call for Data Protection Impact Assessment (DPIA), a systematic analysis of privacy risks at the basis of a comprehensive and detailed characterization of the system. This is often a cumbersome document-driven effort. The Data Protection Modeling Framework (DPMF) supports the creation of a comprehensive model-based description of all data processing activities, involved stakeholders, and affected data subjects, and implements a number of analysis steps essential for meeting accountability requirements.**

In this paper, we demonstrate and highlight the benefits of using a single comprehensive DMPF data protection model and, more specifically, we argue that these models constitute sufficiently detailed and exhaustive views of the system to support: (i) explicit documentation and framing of legal argumentations (e.g., on the different processing purposes and compatibility assessments), (ii) automated and semi-automated verification of core data protection principles, and (iii) generation of appropriate accountability documentation at different levels of detail and customized for different stakeholders such as data subjects or supervisory authorities.

The DPMF tool builds upon the Eclipse Modeling Framework (EMF) and its models are specified in a Sirius Viewpoint Specification. The VIATRA model query engine is used to efficiently traverse and analyze the created models for verification and document generation.

***Index Terms*—GDPR, data protection by design, privacy by design, data protection impact assessment, modeling, tool support**

I. Introduction

The EU General Data Protection Regulation (GDPR) [1] has introduced the notion of Data Protection by Design (DPbD) and, at the same time, refined a number of essential principles to protect data subject's fundamental rights, including privacy and data protection, in the context of the processing of their personal data. The implications of the GDPR go well beyond merely introducing additional requirements in the design and implementation of software systems. It imposes additional constraints on the description of the processing operations and creates the necessity to construct a number of legal arguments well before starting any data processing operation.

One common approach to fulfil that obligation is to perform a Data Protection Impact Assessment (DPIA), which in essence involves creating a description of the data processing activities upon which the evaluation of a number of core principles of the Regulation can be conducted. In order for this activity to reach a certain level of trustworthiness and yield its added value, a systematic and detailed analysis of the data processing activities in light of these principles must be performed.

To support such analysis activities, a number of different tools and methodologies have been proposed, both in academic literature and practice, ranging from questionnaires and checklists [2]–[7] to more structured modeling approaches [8], [9]. There is, however, only limited support for a systematic guidance of compliance assessment exercises.

Beyond these requirements, many different types of information must be communicated to a wide range of stakeholders, such as: (i) data subjects, (ii) national supervisory authorities, (iii) joint controllers, and (iv) processors.

Since they are based on a single, cohesive model, model-based approaches offer a clear benefit over template- or checklist-based approaches in that they can serve as a basis for assistance in these compliance assessments and can be used to generate multiple information exports tailored to these different types of stakeholders.

In this paper, we present and demonstrate the Data Protection Modeling Framework (DPMF), a model-based approach and corresponding modeling tool that provides support for (i) explicitly modeling legal reasonings including risk mitigations; (ii) performing a number of automated and semi-automated legal assessments; and (iii) exporting user-tailored documentation on the data processing operations. We illustrate the implementation of two concrete legal assessments in the current prototype implementation of the DPMF tool.[1]

II. Background and Motivation

In this section, we briefly discuss how the legal and software engineering communities have tackled Data Protection by Design (DPbD), before highlighting some of the gaps inherent to those initiatives. We then outline the main tenets of our approach towards a model-centric, technically- and legally-sound description paradigm that allows systematically addressing legal concerns at the software design stage.

A. A Legal Perspective on Data Protection by Design (DPbD)

Among the general principles enshrined in the GDPR [1], Art. 5(2) entrusts controllers with the responsibility to ensure

[1] More information is available at: https://dpmf.distrinet-research.be/

and demonstrate compliance with the various requirements laid down in the text. More specifically, Art. 24(1) now requires controllers to "*implement appropriate technical and organisational measures to ensure and demonstrate compliance with the Regulation*", while Art. 25(1) compels them to do so "*both at the time of the determination of the means for processing and at the time of the processing itself*".

From a legal perspective, compliance with DPbD usually takes the form of a DPIA. Such an exercise typically consists in: (i) describing and mapping the data processing operations, (ii) identifying and documenting data protection risks, (iii) implementing appropriate technical and organizational countermeasures, and (iv) ensuring a degree of accountability by documenting the assessment process [10]–[13].

Traditional DPIAs are no silver bullet [14]. They are usually performed manually, which requires tremendous effort, can lead to human errors, and incurs considerable overhead to keep it up-to-date with constantly evolving systems.

B. A Software Engineering Perspective on DPbD

Several initiatives in the field of software engineering have attempted to address data protection issues at the early stages of the development life-cycle—during the elicitation of requirements or the establishment of an initial software design.

In that sense, many authors have attempted to translate data protection rules into actionable system requirements, either by streamlining the elicitation of compliance requirements [15]–[18] or by deploying natural language processing techniques [19]–[21]. Others have developed privacy goals and strategies to assist software developers in implementing appropriate countermeasures to reduce the impact of their system on individuals' rights and freedoms [22]–[25]. Finally, some initiatives have extended and adapted risk analysis methodologies to also encompass data protection considerations [7], [11], [26], [27].

There are however, several limitations to these approaches, attributable to several factors [28]: (1) software engineers, who are tasked with the elicitation and implementation of technical countermeasures, and lawyers, who are in charge of interpreting and substantiating data protection rules, in practice operate in a disconnect from each other; (2) no existing architectural approach currently supports performing an exhaustive DPIA in parallel with other design activities, and thus there is no support to make explicit design trade-offs, driven by the outcome and findings of a DPIA; and, (3) current privacy engineering methods have limited support for architecture knowledge management (i.e. maintaining adequate documentation concerning design decisions and their underlying rationale) and this is crucial to meet accountability and demonstrability requirements.

C. A Lack of (Adequate) Tool Support

A fair share of the available guidance on DPIAs is still limited to textual instructions, questionnaires, templates, and checklists to be filled by the controllers [2]–[7], and these suffer from the aforementioned limitations.

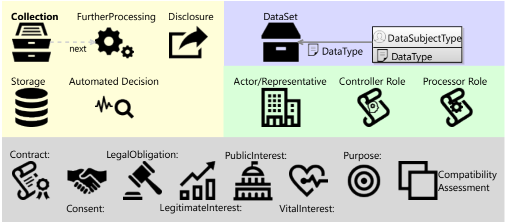


Fig. 1. Legend of the DPM concepts provided by the DPMF.
The top left concepts (in yellow) support the modeling of the collection and further processings. The top right concepts (in blue) model of the involved data sets, data types, and data subject types. The center right (in green) concepts represents the involved actors and the roles. Finally, the bottom row (in gray) shows the concepts to model the six different types of lawful grounds, the purposes, and the compatibility assessments.

While modeling approaches towards GDPR compliance [29]–[31] and tool-support for DPIAs [32], [33] have already been proposed in legal and software engineering literature, those were mostly developed outside of the necessary framing of interdisciplinary legal and software engineering research.

In this context, we have proposed DPMF, a modeling framework that uses key legal abstractions that are typically absent from technical system representations [34] and yet applies techniques and tools adopted from model-driven software engineering and software architecture—the outcome of truly interdisciplinary efforts. The DPMF supports the creation of an accurate description of the system, which in turn is a key enabler towards the (partial) automation of the detection and mitigation of various data protection issues, through: (i) enforcing model constraints, (ii) support for performing legal assessments on the models, and (iii) the extraction of suitable documentation.

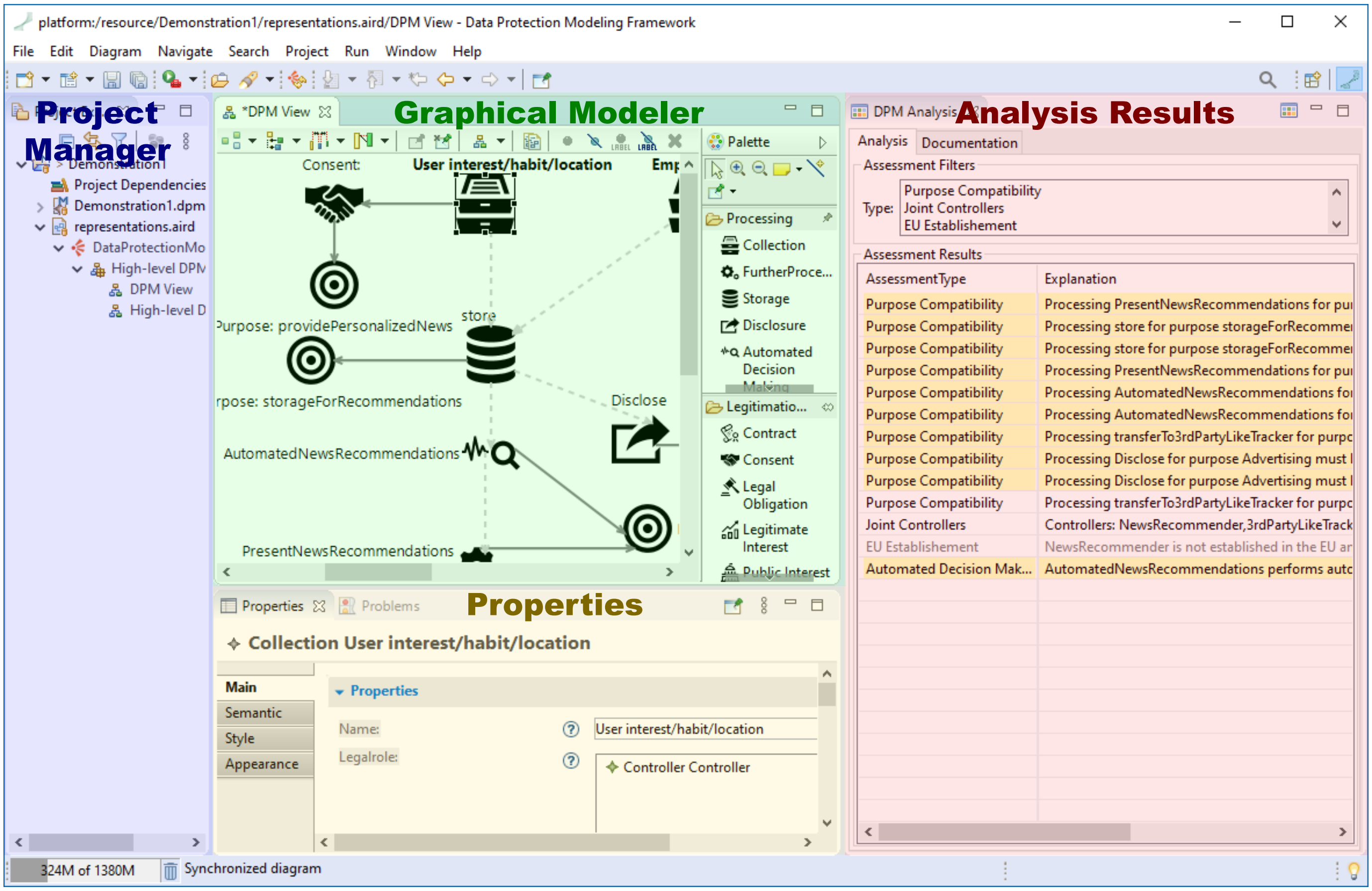
In this article, we present the Eclipse-based prototype implementation of the DPMF designed to assist the modeler when creating a system representation using the modeling framework outlined above.

III. DPMF Implementation

This section first briefly discusses the main components and implementation of the DPMF. Next, it explains the implementation of the different checks and the generation of accountability documentation, based upon queries over the created data protection models.

A. Modeling

The DPMF is implemented as an Eclipse-based product. The support for representing Data Protection Models (DPMs) and the presented concepts (illustrated in Figure 1) is provided by a meta-model [34], implemented in the Eclipse Modeling Framework [35]. The meta-model enforces a number of constraints such as the link between processing operations and the roles that organizations have in them. To create the concrete DPMs, graphical modeling support is implemented using an Eclipse Sirius Viewpoint Specification. This specification provides a high-level visualization which shows the different



Assessment Filters

Type: Purpose Compatibility
Joint Controllers
EU Establishement

Assessment Results

AssessmentType	Explanation
Purpose Compatibility	Processing PresentNewsRecommendations for pu
Purpose Compatibility	Processing store for purpose storageForRecomme
Purpose Compatibility	Processing store for purpose storageForRecomme
Purpose Compatibility	Processing PresentNewsRecommendations for pu
Purpose Compatibility	Processing AutomatedNewsRecommendations fo
Purpose Compatibility	Processing AutomatedNewsRecommendations fo
Purpose Compatibility	Processing transferTo3rdPartyLikeTracker for purp
Purpose Compatibility	Processing Disclose for purpose Advertising must
Purpose Compatibility	Processing Disclose for purpose Advertising must
Purpose Compatibility	Processing transferTo3rdPartyLikeTracker for purp
Joint Controllers	Controllers: NewsRecommender,3rdPartyLikeTrack
EU Establishement	NewsRecommender is not established in the EU ar
Automated Decision Mak...	AutomatedNewsRecommendations performs aut

Collection User interest/habit/location

Main | Semantic | Style | Appearance

Properties

Name: User interest/habit/location

Legalrole: Controller Controller

Fig. 2. Screenshot of the DPMF prototype and its main components.
This screenshot shows the four different panels of the DPMF tool. The left panel (in blue) allows users to manage different modeling projects, files, and visualizations. The top center panel (in green) provides the graphical modeler which enables users to create graphical models of data processing operations. The bottom center panel (in orange) provides the properties of any selected element in the graphical modeler to include additional information on the elements. Finally, the right panel (in red) provides the analysis results of the DPMF on the created model in the center panel and, on a subpanel, provides a number of export options to generate documentation from the model.

elements and their roles, and defers the lower-level details to properties panes (see bottom Figure 2).

The next section discusses the implementation of a number of legal assessments as VIATRA query patterns. These patterns are used both in the different analyses (e.g., verification of data protection principles such as purpose limitation) and documentation generation activities (e.g., record of processing activities). Because of the implementation as model queries, any modifications to the model can efficiently be re-assessed to verify that the identified issues are correctly resolved.

B. Overview of legal assessments and documentation exports

The DPMF implements the following twelve legal assessments (two of which are illustrated in detail in Section III-C): (1) lawfulness, (2) purpose compatibility, (3) data minimization, (4) storage limitation, (5) processing special categories of personal data, (6) processing personal data relating to criminal convictions and offenses, (7) automated decision-making on special categories of data, (8) joint controllers, (9) EU establishment or EU representative, (10) prohibition to engage another processor without controller approval, (11) controller-processor agreement, (12) transfer to third countries.

Additionally, the following four documentation exports are currently implemented:

Compatibility assessment table providing an overview of every processing, the involved personal data, controller, lawful ground, purpose, and compatibility.

Records of processing activities grouping for every organization, the other involved organizations, the purposes, the categories of data subjects and personal data, the time limits, and the processing activities.

Data subject information providing, for every category of data subject, a summary of the relevant data collections, purposes, and controllers.

DPIA report a `docx` export containing all the information in the model that can serve as a template to be further completed for a full-fledged DPIA.

C. Automating Legal Assessments

This section explains the implementation of automated assessments as VIATRA model query patterns. The implementation

```
1 pattern representative(a:Actor) {
2  // actor must be controller or processor
3  Actor.actsAs(a,r);
4  LegalRole(r);
5  // actor is not established in EU
6  Actor.establishedInEU(a,false);
7  // don't find representative
8  neg Actor.representedBy(a,_);
9 }
```

Snippet 1. VIATRA pattern for finding missing representatives.
This VIATRA pattern describes the different criteria for querying a DPM to find all the actors that are not established in the EU and do not have a representative.

of a legal assessment consists of two parts:

Identifying DPM elements. This involves identifying the DPM elements that indicate a potential concern with regard to a specific legal provision that requires a more detailed assessment by a legal stakeholder.

Guiding the mitigation. This step involves guiding the user to determine and instantiate appropriate modifications to the DPM or the implemented organization measures to ensure compliance with the Regulation.

The detection using the model query patterns in VIATRA focuses entirely on the first part above, while any necessary modifications to the model can be directly performed using the graphical editor and via the model elements' properties.

VIATRA uses the concepts presented in Figure 1 as keywords, while properties are separated with a '.' and the parameters are placed between brackets. For example, *Actor.representedBy(actor1, representative1)* is used to express that *actor1* is represented by *representative1*. Combined with *Representative.name(representative1,"TEST")*, this allows us to find all *actor1*'s that have a Representative with the specified name "*TEST*". The *actor1* can thus be matched multiple times, depending on how many actors are represented by a representative with the name "*TEST*".

Below, two examples of DPMF legal assessment patterns are discussed in further detail to illustrate how the concrete models are queried in the DPMF to identify any problematic elements.

1) Representative for controllers or processors not established in the EU: The assessment of representatives for controllers or processors not established in the EU requires the identification of all actors that are not established in the EU and are acting in the legal role of a controller or processor. The pattern shown in snippet 1 shows how to detect all actors with a legal role (lines 3–4), no EU establishment (line 6), and for which no representative can be found (line 8).

2) Find Incompatible Purposes: Another important assessment involves ensuring that the specified purposes of further processing operations are not incompatible with the lawful ground and purpose specified for the collection. The pattern in snippet 2 illustrates how models can be queried for processing purposes incompatible with a collection's lawful ground and purpose (line 1–2) by checking for either the lack of a compatibility (line 4) or an explicit incompatibility (line 6).

```
1 pattern PurposeIncompatible(pp:ProcessingPurpose,
2    c:Collection) {
3  // Either don't find any compatibility
4  neg find Compatibility(pp,c);
5 } or { // or find an explicit incompatibility
6  find Incompatibility(pp,c);
7 }
8 pattern Compatibility(pp:ProcessingPurpose,
9    c:Collection) {
10  // explicit compatibility
11  Collection.subjectTo(c,lg);
12  CompatibilityAssessment.processingpurpose(ca,pp);
13  CompatibilityAssessment.lawfulground(ca,lg);
14  CompatibilityAssessment.compatible(ca,true);
15 } or {
16  // or use the exact same purpose as the collection
17  Collection.subjectTo(c,lg);
18  LawfulGround.purpose(lg,pp);
19 }
20 pattern Incompatibility(pp:ProcessingPurpose,
21    c:Collection) {
22  // find explicit incompatibility
23  Collection.subjectTo(c,lg);
24  CompatibilityAssessment.processingpurpose(ca,pp);
25  CompatibilityAssessment.lawfulground(ca,lg);
26  CompatibilityAssessment.compatible(ca,false);
27 }
```

Snippet 2. VIATRA pattern for finding incompatibilities.
The above three VIATRA patterns describe the different criteria for detecting incompatibilities between the processing purpose specified for the collection (as part of the lawful ground) and the processing purpose of further processing operations. These incompatibilities are retrieved either through a missing compatibility assessment or through an explicit incompatibility *assessment.*

Searching for *compatibilities* (line 8–9), to detect that they are not present, involves finding either: (i) a collection with a lawful ground (line 11) and a compatibility assessment with the purpose (line 12), the lawful ground of the collection (line 13), and a result that specifies they are compatible (line 14); or (ii) the exact same processing purpose as used in the lawful ground of the collection (line 17–18). Finding an incompatibility involves the exact same steps as a compatibility (lines 23–25), but with a negative assessment result (line 26).

IV. Conclusion

We present our tool implementation of the Data Protection Modeling Framework (DPMF) which—currently in prototype phase—allows the creation of comprehensive models of data processing activities. The modeling support of the DPMF is based upon a meta-model that draws upon in-depth knowledge of the GDPR and is the result of interdisciplinary research.

We highlight the following DPMF demonstration scenarios: (i) how it supports the creation of sound and complete models through meta-model and model soundness constraints; (ii) how the DPMF enables a structured, automated and semi-automated verifications vis-à-vis the core principles of the GDPR; and (iii) how the creation of a model representation of the data processing operations enables the generation of accountability documentation tailored to different stakeholders such as data subjects, sub-processors, or supervisory authorities.

The DPMF as presented here is a cornerstone result in our ongoing research towards closer aligning data protection impact assessment (DPIA) activities and practical model-based software engineering methodologies and techniques.

Acknowledgement

This research is partially funded by the Research Fund KU Leuven and the PRiSE KU Leuven-C2 research project.

References

[1] "Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)," *Official Journal of the EU*, 2016.

[2] Article 29 Working Party, "Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of regulation 2016/679 (WP248 rev. 01)," 2017. [Online]. Available: http://ec.europa.eu/newsroom/document.cfm?doc_id=47711

[3] Smart Grid Task Force 2012-14 - Expert Group 2, "Data Protection Impact Assessment Template for Smart Grid and Smart Metering systems," 2018. [Online]. Available: https://ec.europa.eu/energy/sites/ener/files/documents/dpia_for_publication_2018.pdf

[4] European Data Protection Supervisor (EDPS), "Accountability on the ground Part I: Records, Registers and when to do Data Protection Impact Assessments," 2019. [Online]. Available: https://edps.europa.eu/sites/edp/files/publication/19-07-17_accountability_on_the_ground_part_i_en.pdf

[5] ——, "Accountability on the ground Part II: Data Protection Impact Assessments & Prior Consultation," 2019. [Online]. Available: https://edps.europa.eu/sites/edp/files/publication/19-07-17_accountability_on_the_ground_part_ii_en.pdf

[6] European Union Agency for Cybersecurity (ENISA), "On-line tool for the security of personal data processing," 2020. [Online]. Available: https://www.enisa.europa.eu/risk-level-tool

[7] CNIL, "Privacy Impact Assessment (PIA)," Commission Nationale de l'Informatique et des Libertés, 2018. [Online]. Available: https://www.cnil.fr/en/PIA-privacy-impact-assessment-en

[8] A. S. Ahmadian, D. Strüber, V. Riediger, and J. Jürjens, "Supporting privacy impact assessment by model-based privacy analysis," in *Proceedings of ACM SAC 2018: Software Engineering*, 2018.

[9] M. Alshammari and A. Simpson, "A model-based approach to support privacy compliance," *Information & Computer Security*, vol. 26, no. 4, pp. 437–453, 2018.

[10] T. Bisztray and N. Gruschka, "Privacy Impact Assessment: Comparing Methodologies with a Focus on Practicality," in *Secure IT Systems*, A. Askarov, R. R. Hansen, and W. Rafnsson, Eds. Cham: Springer International Publishing, 2019, vol. 11875, pp. 3–19.

[11] S. J. De and D. Le Métayer, "PRIAM: A Privacy Risk Analysis Methodology," in *Data Privacy Management and Security Assurance*. Springer, 2016, pp. 221–229.

[12] F. Bieker, M. Friedewald, M. Hansen, H. Obersteller, and M. Rost, "A Process for Data Protection Impact Assessment Under the European General Data Protection Regulation," in *Privacy Technologies and Policy*, ser. Lecture Notes in Computer Science. Springer, Cham, Sep. 2016.

[13] R. Alnemr, E. Cayirci, L. D. Corte, A. Garaga, R. Leenes, R. Mhungu, S. Pearson, C. Reed, A. S. d. Oliveira, D. Stefanatou, K. Tetrimida, and A. Vranaki, "A Data Protection Impact Assessment Methodology for Cloud," in *Privacy Technologies and Policy*, ser. Lecture Notes in Computer Science. Springer, Cham, Oct. 2015, pp. 60–92.

[14] P. Dewitte, K. Wuyts, L. Sion, D. Van Landuyt, I. Emanuilov, P. Valcke, and W. Joosen, "A Comparison of System Description Models for Data Protection by Design," in *Proceedings of the 34th Symposium on Applied Computing*. Limassol: IEEE, Apr. 2019.

[15] S. Islam, H. Mouratidis, and S. Wagner, "Towards a Framework to Elicit and Manage Security and Privacy Requirements from Laws and Regulations," in *Requirements Engineering: Foundation for Software Quality*, ser. Lecture Notes in Computer Science. Springer, Berlin, Heidelberg, Jun. 2010, pp. 255–261.

[16] A. Siena, A. Perini, A. Susi, and J. Mylopoulos, "A Meta-Model for Modelling Law-Compliant Requirements," in *2009 Second International Workshop on Requirements Engineering and Law*, Sep. 2009, pp. 45–51.

[17] R. Meis, R. Wirtz, and M. Heisel, "A Taxonomy of Requirements for the Privacy Goal Transparency," in *Trust, Privacy and Security in Digital Business*, ser. Lecture Notes in Computer Science. Springer, Cham, Sep. 2015, pp. 195–209. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-319-22906-5_15

[18] R. Muthuri, G. Boella, J. Hulstijn, and L. Humphreys, "Argumentation-Based Legal Requirements Engineering: The Role of Legal Interpretation in Requirements Acquisition," in *Requirements Engineering Conference Workshops (REW), IEEE International*. IEEE, 2016, pp. 249–258.

[19] T. D. Breaux, M. W. Vail, and A. I. Anton, "Towards Regulatory Compliance: Extracting Rights and Obligations to Align Requirements with Regulations," in *14th Intl. Requirements Engineering Conf.*, 2006.

[20] T. Breaux and A. Antón, "Analyzing Regulatory Rules for Privacy and Security Requirements," *IEEE Trans. on Software Engineering*, 2008.

[21] J. C. Maxwell and A. I. Anton, "Developing Production Rule Models to Aid in Acquiring Requirements from Legal Texts," in *2009 17th IEEE International Requirements Engineering Conference*, Aug. 2009.

[22] M. Langheinrich, "Privacy by Design — Principles of Privacy-Aware Ubiquitous Systems," in *Ubicomp 2001: Ubiquitous Computing*, G. Goos, J. Hartmanis, J. van Leeuwen, G. D. Abowd, B. Brumitt, and S. Shafer, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2001, vol. 2201.

[23] M. Rost and K. Bock, "Privacy by Design and the New Protection Goals," *DuD*, vol. 35, no. 1, p. 9, 2011. [Online]. Available: https://www.european-privacy-seal.eu/AppFile/GetFile/ca6cdc46-d4dd-477d-9172-48ed5f54a99c

[24] J.-H. Hoepman, "Privacy Design Strategies," in *ICT Systems Security and Privacy Protection: 29th IFIP TC 11 International Conference, SEC 2014, Marrakech, Morocco, June 2-4, 2014*. Springer, 2014, pp. 446–459.

[25] M. Hansen, M. Jensen, and M. Rost, "Protection Goals for Privacy Engineering," in *2015 IEEE Security and Privacy Workshops*, may 2015.

[26] M. Deng, K. Wuyts, R. Scandariato, B. Preneel, and W. Joosen, "A privacy threat analysis framework: supporting the elicitation and fulfillment of privacy requirements," *Requirements Engineering*, 2011.

[27] L. Sion, D. Van Landuyt, K. Wuyts, and W. Joosen, "Privacy risk assessment for data subject-aware threat modeling," in *2019 IEEE Security and Privacy Workshops (SPW)*. IEEE, 2019, pp. 64–71.

[28] L. Sion, P. Dewitte, D. Van Landuyt, K. Wuyts, I. Emanuilov, P. Valcke, and W. Joosen, "An Architectural View for Data Protection by Design," in *Proceedings of the 2019 International Conference on Software Architecture*. Hamburg: IEEE, Mar. 2019, p. 10.

[29] D. Huth, A. Tanakol, and F. Matthes, "Using Enterprise Architecture Models for Creating the Record of Processing Activities (Art. 30 GDPR)," in *Proceedings of the 23rd IEEE International Distributed Object Computing Conference (EDOC)*, Paris, Oct. 2019, p. 7.

[30] D. Torre, G. Soltana, M. Sabetzadeh, L. C. Briand, Y. Auffinger, and P. Goes, "Using Models to Enable Compliance Checking against the GDPR: An Experience Report," in *Proceeding of the IEEE / ACM 22nd International Conference on Model Driven Engineering Languages and Systems (MODELS 19)*, Munich, Sep. 2019, p. 12.

[31] M. Alshammari and A. Simpson, "A model-based approach to support privacy compliance," *Information & Computer Security*, vol. 26, no. 4, Jan. 2018. [Online]. Available: https://doi.org/10.1108/ICS-11-2017-0084

[32] S. Dashti and S. Ranise, "A Tool-assisted Methodology for the Data Protection Impact Assessment:," in *Proceedings of the 16th International Joint Conference on e-Business and Telecommunications*. Prague, Czech Republic: SCITEPRESS - Science and Technology Publications, 2019, pp. 276–283. [Online]. Available: http://www.scitepress.org/DigitalLibrary/Link.aspx?doi=10.5220/0007932202760283

[33] J. Coles, S. Faily, and D. Ki-Aries, "Tool-Supporting Data Protection Impact Assessments with CAIRIS," in *2018 IEEE 5th International Workshop on Evolving Security & Privacy Requirements Engineering (ESPRE)*. Banff, AB: IEEE, Aug. 2018, pp. 21–27. [Online]. Available: https://ieeexplore.ieee.org/document/8501328/

[34] L. Sion, D. Van Landuyt, P. Dewitte, K. Wuyts, P. Valcke, and W. Joosen, "DPMF: A Modeling Framework for Data Protection by Design," *Enterprise Modelling and Information Systems Architectures*, vol. 15, pp. 10–1, 2020.

[35] D. Steinberg, F. Budinsky, E. Merks, and M. Paternostro, *EMF: eclipse modeling framework*. Pearson Education, 2008.