UNIVERSITY OF TARTU
Institute of Computer Science
Conversion Master in IT

**Kaspar Kala**

# Refinement of the General Data Protection Regulation (GDPR) Model: Administrative Fines Perspective

**Master's Thesis (15 ECTS)**

Supervisors: Raimundas Matulevičius, PhD
Jake Tom

Tartu 2019

## Refinement of the General Data Protection Regulation (GDPR) Model: Administrative Fines Perspective

**Abstract:**

To meet the requirements of the General Data Protection Regulation (2016/679/EU; hereinafter GDPR), organizations need a framework for assessing compliance of their business processes. For such purpose, a Data Protection Observation Engine (hereinafter DPOE) – a software tool enabling business process GDPR compliance check semi-automatically – is created by the researchers of Institute of Computer Science of University of Tartu. Current research on the DPOE has produced a conceptual model covering general GDPR requirements in an UML format describing the key entities, artefacts and relationships between these (hereinafter DPOE Model). The DPOE Model, however, requires validation in terms of legal completeness (i.e. GDPR coverage). The thesis adds to the existing research by legally validating the DPOE Model from the perspective of Article 83(4) and 83(5) of the GDPR concerning administrative fines. These articles describe key GDPR requirements which' infringement bring about fines up to 20,000,000 EUR. Thus, these are the requirements every organization must treat with special attention in order to be compliant with the GDPR. This validation also enables the prime users of DPOE, the data protection officers, to trust the results generated by the DPOE as they know the potential incompliance issues raised are of key importance. This in turn ensures the integrity of the output of the DPOE. As such, the basis for comparing the current version of the DPOE Model to the refined DPOE Model in terms of legal completeness (i.e. GDPR article coverage) is created. In order to measure how legal completeness has in fact improved, the results generated by the refined DPOE Model are compared to the results generated by current version of the DPOE Model on an actual business process (ÕIS2 login process). As a result of the validation and the comparison of the current version of the Model to the refined Model, the maturity of the Model is enhanced.

**Keywords:**

GDPR, compliance, UML, data protection officer, administrative fines.

**CERCS:**

**T120 -** Systems engineering, computer technology

## Isikuandmete kaitse üldmääruse mudeli täiustamine: haldustrahvide vaatenurk

**Lühikokkuvõte:**

Isikuandmete kaitse üldmääruse (2016/679/EL; edaspidi *ÜM*) nõuetele vastamiseks vajavad organisatsioonid raamistikku, mis võimaldab hinnata oma äriprotsesside vastavust ÜM-ile. Sel eesmärgil on Tartu Ülikooli Arvutiteaduste Insituudi teadurid loomas tarkvaralist lahendust, mis võimaldab äriprotsesside vastavust ÜM-ile pool-automatiseerida. Lahenduse nimeks on hetkel pakutud *Data Protection Observation Engine* (edaspidi *DPOE*). Seni tehtud teadustöö on loonud DPOE kontseptuaalse mudeli, mis katab üldisi ÜM-i nõudeid UML formaadis kirjeldades peamisi olemeid, artefakte ja suhteid nende vahel (edaspidi *DPOE Mudel*). DPOE Mudel vajab aga valideerimist ÜM-i täielikkuse aspektist (st. kui palju ÜM-st on kaetud DPOE Mudeliga). Käesolev magistritöö täiendab olemasolevat teadustööd DPOE Mudeli õigusliku valideerimise näol. Valideerimine toimub ÜM artiklite 83(4) ja 83(5) baasil, mis kirjeldab võtmeartiklid, mille rikkumine võib kaasa tüüa rahatrahvid. Selline valideeriline võimaldab DPOE peamistel kasutajatel – andmekaitseametnikel – saada kindlust, et DPOE poolt genereeritud tulemused ja tõstatatud

võimalikud mittevastavused on olulised, kuna need puudutavad võtmeartikleid. See omakorda tagab DPOE tulemuste terviklikkuse. Sellega luuakse ka võimalus võrrelda DPOE Mudeli hetkeversiooni täiustatud DPOE Mudeliga õigusliku täielikkuse (s.t. ÜM artiklite katmise) vaatest. DPOE Mudeli hetkeversiooni ja täiustatud versiooni rakendatakse äriprotsessile (ÕIS2 sisselogimine), et võrrelda, kui palju ÜM-i artikleid Mudelid katavad. Valideerimise ja mudelite rakendamisel äriprotsessile suurendatakse lõpptulemusena DPOE Mudeli küpsust.

**Võtmesõnad:**

Isikundmete kaitse üldmäärus, nõuetele vastavus, UML, andmekaitseametnik, trahvid.

**CERCS:**

**T120** – Süsteemitehnoloogia, arvutitehnoloogia

## Table of Contents

# 1 Introduction

The General Data Protection Regulation (2016/679/EU; *GDPR*) entered into force on 25 May 2018 [1]. Although GDPR is old news since the legal text itself was adopted in 2016, it still generates enough attention and discussions. Although the GDPR steps into the shoes of the Directive 95/46/EU which was adopted in 1995 (*1995 Directive*) [2], the GDPR sets out more stringent administrative fines in case of incompliance (up to 20,000,000 EUR or 4% of the global turnover), introduces new rights to the data subjects (e.g. the right to be forgotten and data portability) and expands its scope of application [3]. However, being the result of a political compromise, the GDPR provides at times generic rules and principles without clear guidance on how certain requirements need to be implemented. Therefore, research has been conducted to represent GDPR in the form of a model in order to aid organizations in achieving compliance and by providing a visual overview for understanding important aspects of the GDPR in UML notation describing the key entities, artefacts and relationships between these (*Model*). Existing research on the Model, however, requires legal validation in terms of legal completeness (i.e. GDPR article coverage) and further testing on an actual business process [4].

Hence, the purpose of the thesis is to: i) validate the Model in terms of legal completeness based on the criteria for refinement and propose modifications thereof; and ii) compare the results generated by the current Model to the results generated by the refined Model using an actual business process to enhance the maturity of the Model. The Model, once tested and validated, will act as the core of the Data Protection Observation Engine (*DPOE*) which is a software tool aiding data protection officer's in their day-to-day operations in helping organizations achieve compliance with the GDPR (thus, the Model will be referred also as *DPOE Model*).

The main research question (**MRQ**) is: **How should the DPOE Model be refined considering the administrative fines?** For answering the MRQ, the criteria for refinement are sought from the GDPR. The current Model is analyzed and based on the limitations thereof, a refined DPOE Model is proposed. Thereafter, the legal completeness (i.e. GDPR article coverage) of the current DPOE Model is compared to the refined DPOE Model. Lastly, the feasibility of the refined and current DPOE Models is compared on an actual business process model.

**SUBQ1**: **What are the criteria for refining the DPOE Model?** Section 2 focuses on defining and explaining the criteria for refinement of the DPOE Model. The criteria chosen are the administrative fines set out in Articles 83(4) and 83(5) of the GDPR.

**SUBQ2**: **What is the legal completeness (i.e. GDPR article coverage) of the current DPOE Model compared to the refined Model considering the criteria of refinement?** Sections 3 and 4 provide an overview of the coverage of the GDPR articles by both the current and refined DPOE Models. The coverage of the two Models is then compared to conclude which of the Models provides greater legal completeness (i.e. GDPR article coverage) in terms of avoiding administrative fines.

**SUBQ3**: **What is the feasibility of the refined DPOE Model?** Section 5 applies the current and the refined DPOE Models to a running business process example to instantiate the two Models and compare the results generated by both DPOE Model applications.

The thesis follows the method set out in Figure 1. Firstly, the criteria for refining the current DPOE Model are established (section 2). The criteria for refinement will be based on the severity of fines set out in Articles 83(4) and (5) of the GDPR. Thereafter, the current Model is evaluated, and the limitations of the current Model are detected based on the criteria of

refinement (section 3). The results of the evaluation together with the criteria for refinement will serve as an input for the next step, which is the modification of the DPOE Model (section 4). As a result of section 4, a modified DPOE Model is proposed (section 4.1). Thereafter, the refined Model and the current Model are tested on a business process model for insights (section 5.2). These insights will be the input for comparing the two Models based on the criteria for refinement (section 5.3). As a result, it is possible to conclude whether the refinement process increased the GDPR article coverage and whether the refined Model helps organizations better avoid administrative fines under the GDPR(section 6).

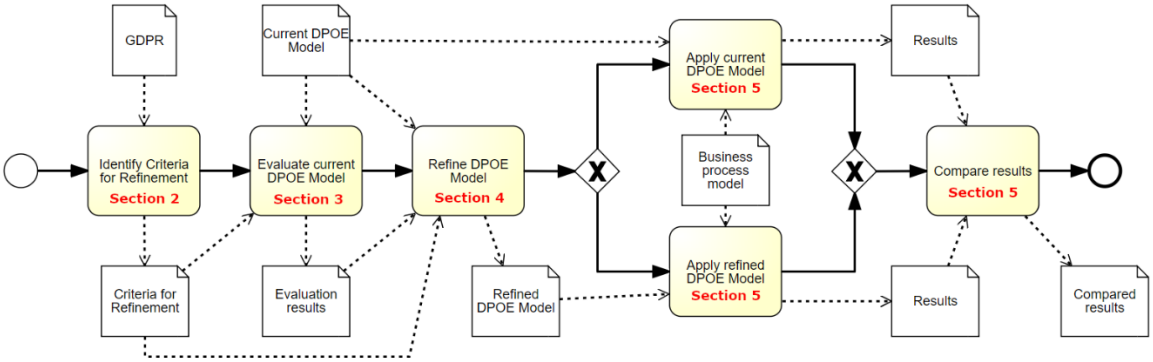


**Figure 1.** Research method

# 2 Background

The purpose of this section is to identify the criteria for refinement of the DPOE Model. In 2.1, the key GDPR articles together with the criteria of refinement are explained and defined. Section 2.2 lists competing research that is relevant for this thesis.

## 2.1 Protection of Personal Data in the European Union

### 2.1.1 Protection of Personal Data in Primary EU Law

The right to data protection of personal data became a legally binding right in primary EU law in 2009 after the entering into force of the Lisbon Treaty [5, p. 28]. The Lisbon Treaty made the originally political document of Charter of Fundamental Rights of the European Union (*EU Charter*) a legally binding instrument. Article 8 of the EU Charter raises the right to personal data protection to the level of a fundamental right in EU law. Article 8(1) of the EU Charter explicitly mentions the right of personal data protection being a fundamental right. Article 8(2) of the EU Charter refers to key data protection principles, while Article 8(3) requires an independent authority to control the implementation of the data protection principles [5].

Besides being elevated to fundamental right status in the EU Charter, the right to personal data protection is also listed in Article 16 of the Treaty of the Functioning of the EU (*TFEU*) under the chapter of general principles. As such, Article 16 of the TFEU creates a legal basis for the EU institutions to legislate on data protection matters [5]. This is an important step because although the 1995 Directive was adopted 14 years earlier, its legal basis was not the protection of personal data of EU citizens, but the free movement of personal data in the internal market (Article 100a of the Treaty establishing the European Community [6]). As such, Article 16 of the TFEU served as a legal basis for the GDPR [7, p. 29].

### 2.1.2 General Data Protection Regulation (GDPR)

As mentioned above, the predecessor of the GDPR was the 1995 Directive. Being a directive, it meant that it needed to be transposed to national laws of the EU Member States. In practice, that meant that instead of a single data protection regime in Europe, the legal landscape was fragmented and applied to a different degree as Member States had a margin of discretion. Although the 1995 Directive was a full harmonization directive, it was not transposed similarly across the EU [7, p. 30]. Besides this, it was argued that the 1995 Directive did not meet the challenges of the 21st century as means for data processing had been developing rapidly since the adoption of the 1995 Directive. Mayer-Schönberger and Padova point out that the 1995 Directive was negotiated at the time "when the Internet was still little more than a niche network, connecting mainframes, minicomputers and a small but growing number of PCs through slow dialup connections. Smartphones did not exist, storage space was measured in megabytes, e-commerce was just being born, and widespread social media was science fiction" [8]. Being outdated and without a harmonizing effect were the main reasons prompting the EU data protection reform which led to the adoption of the GDPR in 2016 [7, p. 30].

The GDPR is seen as fit for purpose for protecting the fundamental right to personal data protection in the digital age by some [7, p. 30], but has also received criticism due its limiting nature for conducting Big Data analysis [9,10]. The limitations of the GDPR are, however, out of scope of this thesis.

The GDPR preserves much what the 1995 Directive already sets out (e.g. the core principles and rights of the data subject) while at the same time introduced new obligations requiring

organizations to implement data protection by design and by default; to appoint a data protection officer in certain circumstances; to comply with a new right to data portability; and to comply with the principle of accountability [7, p. 30].

#### 2.1.2.1 Administrative Fines – Criteria for Refinement

One of the critical aspects for controllers and processors has been the significant increase in fines when data protection rules are not complied with. This has meant that data protection compliance needs to be taken more seriously. Supervisory authorities are given the right to issue administrative fines up to 20,000,000 EUR or 4% of global turnover in case of certain infringements.

The GDPR sets out a tiered approach to fines [7, p. 248]. The supervisory authorities have the mandate to issue: a) fines up to 20,000,000 EUR or 4% of the global turnover whichever is higher under Article 83(5) of the GDPR; or b) fines up to 10,000,000 EUR or 2% of the global turnover whichever is higher under Article 83(4) of the GDPR.

Article 83(5) of the GDPR includes infringements of the basic principles of processing and the conditions for consent (Articles 5, 6, 7 and 9), breaches of data subjects' rights (Articles 12-22) and of the regulation's provisions governing the transfer of personal data to recipients in third countries (Articles 44-49) [7, p.248]. Article 83(4) of the GDPR makes punishable infringements that include obligations of the controller and the processor (Articles 8, 11, 25-39, 42 and 43), obligations of the certification body (Articles 42 and 43) and obligations of the monitoring body (Article 41(4)).

As the aim of the thesis is to refine the DPOE Model and helping organizations to avoid fines and be compliant with the GDPR, the administrative fines are the basis for current DPOE Model refinement.

**Table 1.** GDPR articles forming the criteria for refinement for the current DPOE Model

| **Up to 10,000,000 EUR fine (Article 83(4) of the GDPR)** | **Up to 20,000,000 EUR fine (Article 83(5) of the GDPR)** |
|---|---|
| Article 8 | Article 5 |
| Article 11 | Article 6 |
| Articles 25-39 | Article 7 |
| Article 41(4) | Article 9 |
| Article 42 | Articles 12-22 |
| Article 43 | Articles 44-49 |

Articles set out in Table 1 are key for organizations aiming to be compliant with the GDPR. Failure in doing so constitutes infringement and may bring about the obligation to pay administrative fines. Thus, the articles of Table 1 provide the purpose to the DPOE Model refinement process – avoiding fines and achieving compliance.

#### 2.1.2.2 Key Terminology

Regarding the material scope of the GDPR, key terms must be identified first. These are set out in Article 4 of the GDPR.

"Personal data" means any information relating to an identified or identifiable natural person ('data subject'; [1, art. 4(1)]). Furthermore, the same article explains that "an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person." The GDPR stipulates that "to determine whether a natural person is identifiable, account should be taken of all the means reasonably

likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments [1, recital 26].” Therefore, the GDPR sets out a reasonable likelihood test taking not only into account the subjective ability to identify a natural person, but the state of the art of the technology [11]. Thus, a piece of data could be anonymous (information that does not relate to an identified or an identifiable natural person [1, recital 26]) at the time of collection but could later be personal data due to the technological advancements [11, p. 5]. As such, the term “personal data” must be understood in a broad manner [12].

A sub-category of personal data is “special categories of personal data”. Special categories of personal data are data “revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health, data concerning sex life or sexual orientation [1, art. 9(2)]”. The general rule is that the processing of special categories of data is prohibited, unless an exception exists under [1, art. 9(1), 9(2)]. As special categories of data merit more protection, special requirements must be adhered to when such data is processed. Another type of special category of personal data is described in Article 10 of the GDPR - “personal data relating to criminal convictions and offences or related security measures”. Although not listed in Article 9 of the GDPR, this data is also considered as data requiring more protection and is often approached similarly in the GDPR (see [1, art.27(2)(a), 30(5)]).

Another key term in the context of GDPR is “processing”. The term “processing” is a broad term covering “any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction [1, art. 4(2)]”. The use of “such as” refers to the fact that it is an open list of examples. According to Article 2(1) of the GDPR, the GDPR applies to the processing of personal data “wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system (means “any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis [1, art. 4(6)]”.

The parties conducting processing of personal data are the “controller” and the “processor”. Controller is a “natural or legal person, public authority, agency or other body which, alone or jointly with others (joint-controllers), determines the purposes and means of the processing of personal data [1, art. 4(7)]”. Processor is a “a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller [1, art. 4(8)]”. The concept of controller is primarily important in terms of responsibility [13]. The relationship between controller and processor must be either regulated by a contract or a legal act [1, art.28(3)].

#### 2.1.2.3 Key Principles

Principles relating to the processing of personal data are set out in Article 5 of the GDPR. It highlights seven principles that must be applied cumulatively.

**Principle of lawfulness, fairness and transparency:** This means that the processing of personal data must have a legal base and the processing must be conducted in a transparent and fair manner.

**Principle of purpose limitation:** This obliges the controllers and processors to process personal data under specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Further processing is permitted in limited cases for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) of the GDPR. Article 6(4) of the GDPR sets out the criteria to follow when deciding whether a new processing activity is compatible with the initial purpose if the new processing activity is not based with consent or EU or Member State law.

**Principle of data minimization:** Under this principle, the personal data processed must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. Thus, controllers and processors should only attain data that is strictly necessary for the purposes of the processing undertaken.

**Principle of accuracy:** This principle mandates controllers to process only accurate and, where necessary, up to date personal data. Controllers must take every reasonable step to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without undue delay.

**Principle of storage limitation:** This means that personal data should be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. Exclusions exist for archiving, scientific or historical research purposes or statistical purposes provided that appropriate technical and organizational measures are implemented.

**Principle of integrity and confidentiality:** Under this principle, the personal data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures.

**Principle of accountability:** Under this principle, the controller is not only responsible for the breaches under the GDPR but must also be able to demonstrate compliance with GDPR in its everyday processes. Compared to the 1995 Directive, this is a new principle. It obliges controllers to take concrete and practical measures to protect the fundamental right to data protection of the data subjects [14].

#### 2.1.2.4 Lawfulness of Processing Personal Data

The GDPR describes six legal grounds under which personal data may be processed. As stipulated by the principle of lawfulness [1, art. 5(1)(a)], the processing of personal data is lawful only if there is a legal base.

**Consent:** One of the legal bases in the GDPR is consent [1, art. 6(1)(a)]. Although it is listed as the first in the list of legal grounds in Article 6, it is by no means the most important legal ground or the best one. Consent has many requirements that need to be met. Firstly, consent needs to be freely given, specific, informed and unambiguous indication of the data subject's wishes. “Freely given” means that it must be a real choice for data subject [15]. “In order to ensure that consent is freely given, consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller, in particular where the controller is a public authority and it is therefore unlikely that consent was freely given in all the circumstances of that specific

situation [1, recital 43]". Consequently, public sector should generally not rely on consent as a legal basis as it is presumed that it would constitute imbalance and, therefore, not be freely given. Similarly, consent in the employer-employee context is not generally considered as freely given [15]. Also, Article 7(4) of the GDPR indicates that, inter alia, the situation of "bundling" consent with acceptance of terms or conditions, or "tying" the provision of a contract or a service to a request for consent to process personal data that are not necessary for the performance of that contract or service, is considered highly undesirable. If consent is given in this situation, it is presumed to be not freely given [15]. One other aspect in deciding whether consent is freely given is the aspect of detriment. This means that the controller needs to prove that withdrawing consent does not lead to any costs for the data subject and no clear disadvantage for those withdrawing consent [15]. The controller must be able to prove that consent was provided freely according to principle of accountability [1, art. 5(2)].

Besides the aspect of freedom or genuine choice, the aspects of specificity, unambiguousness and providing enough information need to be fulfilled. Specificity refers to the fact that the purpose of processing must be clearly stated. It also refers to the aspect that consent is sought in terms and conditions, it must be clearly separated from other aspects [15].

The GDPR also sets out the requirement that consent must be informed. This means that at least the following aspects need to be covered in order the data subject could provide an informed consent: i) identity of the controller; ii) purpose of each processing operation consent is sought for (1, recital 42); iii) what (type of) data will be collected and used; iv) the existence of the right to withdraw consent (under Article 7(3), the data subject has always the right to withdraw consent; withdrawing consent has no retroactive effect); iv) information about the use of the data for automated decision-making in accordance with Article 22 (2)(c) of the GDPR where relevant; and (vi) possible risks of data transfers due to absence of an adequacy decision and of appropriate safeguards as described in Article 46(3) of the GDPR.

Besides the requirements above, the consent needs to be unambiguous. This means that the consent needs to be presented as an affirmative action. The data subject must have taken a deliberate action to consent to the processing (e.g. ticking a box) [15]. Inaction such as the use of pre-ticked boxes or consenting via default browser settings fail to meet this requirement.

All in all, these requirements set clear boundaries and limitations on the use of consent.

**Contract:** One separate legal ground is processing of personal data necessary for the performance of a contract to which the data subject is a party [1, art. 6(1)(b)]. This includes the steps taken at the request of the data subject prior to entering into a contract [1, recital 44]. Thus, processing personal data for the conclusion and the performance of the contract (e.g. an employment agreement) does not require any extra grounds (like consent) and is legal in itself considering the data processing principles described above (e.g. data minimization and purpose limitation). According to the United Kingdom's Information Commissioner, the notion of "necessary for" implies that the processing must be necessary to deliver the controller's side of the contract with a natural person. If the processing is only necessary to maintain the business model of the controller more generally, this lawful basis will not apply, and another lawful basis should be considered [16].

**Compliance with a Legal Obligation:** Processing of personal data is lawful if it is processed by a private entity in order to comply with a legal obligation to which the controller is subject [1, art. 6(1)(c)]. The legal obligation must be laid down in EU or Member State

law the controller is subject to [1, art. 6(3)]. For example, financial institutions are obliged to follow know-your-customer (KYC) regulations. Thus, data that the financial institutions are gathering and processing to meet the KYC rules set out in Member State or EU laws rely on Article 6(1)(c) as a legal base.

**Vital Interests of a Natural Person:** Processing of personal data is lawful if it is necessary to protect the vital interests of the data subject or of another natural person [1, art. 6(1)(d)]. As this suggests, this ground may only be invoked if the vital interests (e.g. taking a blood sample without the consent of the patient if the patient is unconscious to discover if the patient may undergo specific procedure to save his/her life) are at stake. If vital interest of the data subject are not at stake, personal data may not be processed under this legal ground.

**Public Interest or the Exercise of Official Authority:** This ground of processing must be laid down in EU or Member State law. It states that processing is lawful, if it is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller [1, art. 6(1)(d)]. It is the main source of processing for government entities. Case-law from the European Court of Justice (*CJEU*) suggests that the word "necessary" means that the data processed must be strictly necessary to perform the public task [17, para. 54, 58-59, 66-68]. The CJEU has stated, for example, that the purpose of "fighting crime" necessarily involves "the prosecution of crimes and offences committed, irrespective of the nationality of their perpetrators" [17, para. 78].

**Legitimate Interests:** Under this ground, processing of personal data is permitted, "if it necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child [1, art. 6(1)(f)]". As stated in [1, recital 47], the existence of legitimate interest must be assessed carefully in each specific case and a balancing act must be conducted between the interests of the controller and the interests or fundamental rights and freedoms of the data subject. [1, recital 47] also stipulates two examples which could be considered as a "legitimate ground" – processing personal data for the purposes of preventing fraud and the processing of personal data for direct marketing purposes. However, this should not be read in a manner that direct marketing or fraud detection could always be considered legitimate grounds for processing. Only after careful consideration and the conduction of a balancing act by the controller could this conclusion be reached. It must be noted that this ground extends only to the data that is strictly necessary for such a purpose (e.g. fraud detection).

This legal ground does not apply to the processing of personal data by public authorities in the performance of their tasks [1, recital 47]. Article 29 Working Party has indicated in its opinion that the principles of accountability and transparency are crucial in the exercise of this legal ground. Therefore, the balancing act should be documented, and it should be presentable to a supervisory authority upon request [18].

#### 2.1.2.5 Data Subject's Rights and Enforcement

Articles 13 to 21 of the GDPR set out the rights of the data subject. In general, these rights have not changed since the 1995 Directive with a few exceptions. Namely, the "right to be forgotten" (Article 17) and the right to data portability (Article 20).

Under the GDPR, the data subject has eight distinctive legal rights which will be described in brief below.

**The Right to be Informed***:* Articles 13 and 14 of the GDPR provide a list of information that need to be presented to the data subject if the data is collected from the data subject or otherwise. These articles describe the content of terms and conditions regarding data processing and is, as such, a key transparency requirement under the GDPR. Information that needs to be provided include name and contact details of the controller, the purpose(s) of processing, the lawful basis for processing, data retention period, the right to lodge a complaint to a supervisory authority, information about the right to withdraw consent (if applicable) and the right to object. The information needs to be provided in concise, transparent, intelligible and easily accessible form, using clear and plain language [1, art. 12(1)].

**The Right of Access:** Data subjects have the right to receive a copy of their personal data as well as other supplementary information [1, art.15(1), 15(3)]. The data subject has the right to receive information about the purpose(s) of processing, the categories of personal data concerned, the recipients or categories of recipient to whom the personal data have been or will be disclosed, data retention period (if possible), the right to lodge a complaint with a supervisory authority, the existence of automated decision-making, including profiling. While exercising the right of access, rights and freedoms of other data subjects may not be adversely affected [1, art. 15(4)].

**The Right to Rectification:** Data subjects have a right to have inaccurate personal data rectified or completed if it is incomplete [1, art. 16]. The controller needs to respond within a calendar month.

**The Right to be Forgotten:** The "right to be forgotten" or the right of erasure as it is stipulated in [1, art.17], was much disputed even prior to the adoption of the GDPR due to the *Google Spain* [19] case in the CJEU where the right to be forgotten was enforced on the basis 1995 Directive. Although contentious, it is in fact not an absolute right and its scope of application is fairly narrow. The right is applicable only if, for example, the data subject withdraws consent on which the processing is based and where there is no other legal ground for the processing, or the personal data have been unlawfully processed [1, art. 17(3)]. One cannot have oneself deleted from a population or any other government registry that is established in the public interest or where the data is necessary for exercising the right of freedom of expression and information under the right to be forgotten.

**The Right to Restrict Processing:** Data subjects have, under certain circumstances, the right to request the restriction [1, art. 4(3)] or suppression of their personal data [1, art. 18]. When processing is restricted by the data subject, the controller is permitted to store the personal data, but not use it [1, art. 18(2)].

**The Right to Data Portability:** A new right under the GDPR – the right to data portability – enables data subjects to obtain and reuse their personal data in a machine-readable format for their own purposes across different services. However, this does not apply to all data and all sectors. The right can be enforced only where the data processing is based with consent [1, art. 20(1)(a)]. Besides these limitations, the GDPR sets out that the right to data portability exists only where it is technically feasible [1, art. 20(2)]. This means that a service provider can always invoke this ground and say it is not feasible.

As was the case with the right to be informed, exercising the right to data portability may not adversely affect the rights of other data subjects [1, art. 20(4)].

**The Right to Object:** Data subject has the right to object to the processing of his or her data when his or her data is processed by a public sector entity for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller

or by a private sector entity for the purposes of the legitimate interests pursued by the controller or by a third party [1, art 21(1)]. When personal data is processed for direct marketing purposes, the data subject has always the right to object [1, 21(2)].

The effect of objection is that the controller is obliged to stop processing of personal data.

**Rights in relation to Automated Decision-Making and Profiling:** The data subject has the right not to be subject to a decision based solely on automated processing, including profiling [1, art. 4(4)], which produces legal effects concerning him or her or similarly significantly affects him or her [1, art. 22(2)]. Automated decision-making, including profiling, is permitted if it is necessary for the entry into or performance of a contract, authorized by Union or Member state law applicable to the controller or based on the individual's explicit consent. Automated decision-making should not be based on special categories of data, unless such decisions are based on explicit consent of the data subject or making such decision is necessary for reasons of substantial public interest as set out in [1, art. 9(2)(g)].

#### 2.1.2.6 International Data Transfers under GDPR

Chapter V of the GDPR sets out the requirements to be followed when personal data is transferred to third countries or international organizations. It is important in the context of this thesis as the transfer of data to countries outside EU (third countries) requires a specific legal base stipulated in the GDPR. It is important to note that data transfers between EU countries do not require any authorizations as the level of personal data protection is high and harmonized by the GDPR.

The rules on international data transfers can be divided into four: i) transfers to countries (but also territories or sectors) which have an adequacy decision from the European Commission; ii) transfers on the basis of appropriate safeguards; iii) transfers on the basis of binding corporate rules; and iv) transfers of data based on derogations from [1, art. 44].

**Data Transfers Based on Adequacy Decisions:** Transfers of personal data to a country, territory or sector that is deemed to have adequate level of protection of personal data by the European Commission, are without any restrictions [1, art. 45(1)]. This means that data transfers to an entity with an adequacy decision is like transferring data to another EU Member State. Adequacy decisions granted will be continuously monitored by the European Commission. As of 6 January 2019, the European Commission has made twelve adequacy decisions [20].

**Data Transfers Based on Appropriate Safeguards:** In the absence of an adequacy decision, personal data may be transferred to a third country or an international organization by the controller or processor if they have provided appropriate safeguards and on condition that enforceable data subject rights and effective legal remedies for data subjects are available [1, art. 46(1)]. Such appropriate safeguards may be provided for in, for example, standard data protection clauses adopted by the European Commission, binding corporate rules or a legally binding and enforceable instrument between public authorities or bodies [1, art. 46(2)]. Such safeguards do not require an authorization from the supervisory authority [1, art. 46(1)]. In certain scenarios, the authorization of the supervisory authority, however, is applicable [1, art. 46(3)].

**Data Transfers Based on Binding Corporate Rules:** GDPR allows for personal data transfers based on binding corporate rules for international transfers that take place within the same group of enterprises or undertakings that are part of a joint economic activity [7, p.262]. Binding corporate rules need to be approved by a competent supervisory authority [1, art. 47(1)].

**Derogations:** In limited cases, the GDPR permits international data transfers in the absence of an adequacy decision, appropriate safeguards or binding corporate rules. The GDPR sets out seven exceptions where international data transfer may be permitted [1, 49(1)]. For example, when the data subject has explicitly consented the data transfer after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards. Public authorities in the exercise of their public powers may not rely on consent for international data transfers [1, art. 49(3)].

#### 2.1.2.7 Information Security Requirements

Information security-related requirements are set out in Articles 32-34 of the GDPR. As noted above, data confidentiality and integrity are one of the key principles of the GDPR. Therefore, information security is something that the controllers and processors need to apply to be in conformity with the GDPR.

**Security of Processing:** The GDPR sets out that the principle that the controller and the processor must implement appropriate technical and organizational measures to prevent any unauthorized interference with data processing operations [1, art. 32(1)]. In deciding what is appropriate, the following aspects need to be considered: a) the security features available in the market for any processing; b) the costs; and c) the risks of processing the data for fundamental rights and freedoms of data subjects [7, p. 165]. The GDPR also lists potential security measures that could be considered appropriate measures: a) pseudonymization [1, art. 4(5)] and encryption of personal data; b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing [1, art. 32(1)].

While assessing the appropriate level of security, account must be taken of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed [1, art 32(1)].

These general rules on information security comprise the information security requirements set out in the GDPR. As one can deduce, these are not case-specific and need to be narrowed down for each system and processing activity. What is also clear is that the GDPR does not only focus on technical measures, but also highlights the importance of organizational measures (i.e. access rights, division of responsibilities) to achieve data security [1, art. 32(1)].

**Data Breach:** A personal data breach [1, art. 4(12)] refers to a security breach leading to the accidental or unlawful destruction, loss, alteration or unauthorized disclosure or access to processed personal data [1, art. 4(12)]. The criteria that need to be adhered to when a personal data breach occurs are set out in [1, art. 33]. The controller needs to notify the supervisory authority within 72 hours after having become aware of the breach. However, this does not apply when the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. The GDPR also sets out the minimum information requirements for a data breach notification [1, art. 33(3)]. The notification must include, at least, a description of the nature of the data breach and of the categories and approximate numbers of data subjects affected, a description of the possible consequences of the breach and of the measures implemented by the controller to address and mitigate its consequences. In addition, the name and contact details of the data protection officer or another contact point

should be provided, to enable the competent supervisory authority to obtain further information if necessary [7, p.173]. Data breaches, its effects and remedial actions taken need to be documented by the controller to enable the supervisory authority verify compliance [1, art. 33(5).

In some cases, the GDPR obliges controllers to communicate data breach information to the data subjects. This is obligatory when the breach is likely to result in a high risk to the rights and freedoms of natural persons [1, art. 34(1)]. The controller must communicate, in plain language, the same information that needs to be submitted to the supervisory authority, except the description of the nature of the data breach and of the categories and approximate numbers of data subjects affected. Communication to the data subjects does not need to be undertaken when: a) the controller has implemented appropriate technical and organizational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorized to access it, such as encryption; b) the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialize; and c) it would involve disproportionate effort [1, art. 34(3)].

#### 2.1.2.8 Accountability Requirements

To ensure accountability in the processing of personal data, controllers and processors must maintain records of the processing activities carried out under their responsibility and provide them to the supervisory authorities when requested. Also, the GDPR puts forward several instruments for promoting compliance, such as the appointment of data protection officers in certain situations, conducting a data protection impact assessment before commencing data processing activities which are likely to pose high risks to the rights and freedoms of individuals and prior consultation with a relevant supervisory authority if the data protection impact assessment indicates that processing presents risks that cannot be mitigated.

**Record of Processing Activities:** The GDPR sets out the obligation to maintain a record of processing activities that shall contain information about: a) name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer; b) purposes of the processing; c) description of the categories of data subjects and of the categories of personal data; d) categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organizations; e) where applicable, transfers of personal data to a third country or an international organization, including the identification of that third country or international organization; f) where possible, the envisaged time limits for erasure of the different categories of data; and g) where possible, a general description of the technical and organizational security measures applied [1, art. 30(1)]. The records may be stored either on paper or electronically [1, art. 30(3)] and must be made available to a supervisory authority upon its request to demonstrate compliance [1, art 30(4)].

**Appointment of a Data Protection Officer (*DPO*):** The DPO's task is to advise the controller in terms of GDPR requirements, monitor compliance, raise awareness and co-operate with the supervisory authority [1, art. 39(1)]. The DPO must directly report to the highest management level [1, art. 38(3)].

Although dealing with GDPR compliance, the DPO itself is not responsible for compliance and the responsibility vests in the controller. The designation of a DPO is compulsory if: a) the processing is carried out by a public authority or body (excluding courts acting in their

judicial capacity); b) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or c) the core activities of the controller or the processor consist of processing on a large scale of special categories of data and personal data relating to criminal convictions and offences [1, art. 37(1)]. The DPO may be a staff member of the controller or processor or fulfil the tasks based on a service contract [1, art. 37(6)]. The contact details of the DPO need to be public and communicated to the supervisory authority [1, art. 37(7)] as they deal with cases and data subject's request from both inside the organization and outside.

The DPO may not receive instructions from the management of the controller regarding the exercise of his or her tasks [1, art. 38(3)]. Also, he or she may not be dismissed or penalized by the controller or the processor for performing his or her tasks as a DPO. The DPO is bound by secrecy or confidentiality concerning the performance of his or her tasks [1, art. 38(5)].

When co-operating with the supervisory authority, the DPO is responsible for prior consultation (see below) and data breach notification procedure described above.

**Conducting a Data Protection Impact Assessment (DPIA) and Prior Consultation with a Supervisory Authority:** The GDPR introduces a new type of self-assessment risk-management procedure that needs to be conducted if a certain type of processing, in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons [1, art. 35(1)]. In such a case, prior to the processing, the controller needs to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. In three scenarios, the conduction of a DPIA is obligatory under the GDPR: a) a systematic and extensive evaluation of personal aspects relating to natural persons is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person; b) large scale processing of special categories of data, or of personal data relating to criminal convictions and offences is undertaken; and c) a systematic monitoring of a publicly accessible area on a large scale [1, art 35(3)].

According to the GDPR, the DPIA needs to include at least a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller; an assessment of the necessity and proportionality of the processing operations in relation to the purposes; an assessment of the risks to the rights and freedoms of data subjects; and the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with the GDPR taking into account the rights and legitimate interests of data subjects and other persons concerned [1, art. 35(7)].

If, as a result of the DPIA, some risks remain unmitigated, the controller is obliged to consult with a supervisory authority. In return, the supervisory authority is obliged to give written advice how to achieve compliance with the GDPR within eight weeks from the date of receiving the request for consultation [1, art. 36].

**Data Protection by Design and by Default:** The GDPR sets forward an obligation for a controller to implement and integrate appropriate technical and organizational measures (e.g. pseudonymization and data minimization) to meet the requirements of the GDPR and protect the rights of the data subjects (i.e. data protection by design) [1, art. 25(2)]. These measures should be implemented both at the time of processing and when determining the means for processing. In implementing these measures, the controller needs to consider the

state of the art, the costs of implementation, the nature, scope and purposes of personal data processing and the risks and severity for the rights and freedoms of the data subject [7, p. 183].

Also, the controller must implement appropriate technical and organizational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed (i.e. data protection by default) [1, art. 25(2)].

### 2.2 Related Works

This section introduces relevant competing research in relation to GDPR representation.

The French Data Protection Authority (*CNIL*) has created an open source software DPIA tool to help controllers and processors meet the requirements of Article 35 of the GDPR [21]. It helps controllers and processors fill in the gaps to compose a DPIA both from the context perspective (e.g. processing activities, purposes), legal perspective (how are the data protection principles followed), risk perspective (how are certain risks mitigated) and validation (risk scores and action plan for mitigation). Thus, the CNIL DPIA tool focuses on conducting the DPIA, not providing a model for the GDPR.

Robol et al. propose a GDPR modelling framework for supporting the design of GDPR compliant systems [22]. Robol et al. present a goal-based modelling language to model the social aspects of the GDPR and the relationships between the different actors using the socio-technical security (STS) method and extend it to GDPR needs with STS-ml. Further formalization of the STS-ml language will be needed to specify other constrains imposed by the GDPR.

Diamantopulou et al. propose a meta-model to derive privacy level agreements (PLAs) for e-government services [23]. PLAs are like service level agreements specifically tailored towards the privacy domain. The authors argue that PLA adoption will enhance citizens' trust since there is a formal agreement that guarantees that citizens privacy preferences are respected. Future work includes the identification of appropriate methods and tools that will enable public authorities to capture the necessary information during the design time of the public authority's system and to support run-time privacy protection.

Becker et al. introduce a meta-design for integrating regulatory requirements into the information system development process to ensure legal compliance [24]. The meta-design aims to be applicable to any regulation and is represented as a four-field matrix that describe four perspectives that must be considered in order to account for regulations. This research does not explicitly deal with the modelling of data protection rules but could be used as a reference model.

Celebi has used Secure Tropos methodology to model GDPR requirements from the goal and rule perspective with Privacy Enhanced Secure Tropos (PESTOS) [25]. The work proposes a meta-model for GDPR compliance in UML and a PESTOS meta-model. Future work would contain validation as the current level of privacy modelling is scarce.

Sing proposes a methodology for analyzing business processes of information systems and aligning them with the GDPR [26]. Sing proposes an UML model of the GDPR, a methodology for GDPR compliance analysis using business process models in BPMN and the outline of the software tool that could take a BPMN model as an input and receive recommendations based on GDPR compliance or incompliance. Future work includes legal validation and prototype improvements. The same model has been used by Tom et al. in [4]. The same model is used as the major input for this thesis and will be refined based on criteria for refinement defined in 2.1.2.1.

## 2.3 Summary

This section defined the criteria for refining the current DPOE Model which are demarcated by Articles 83(4) and 83(5) of the GDPR. In lay terms, the DPOE Model will be refined based on GDPR requirements which' infringement by controllers and processors may bring about the obligation to pay fines.

Section 2.1 set out the criteria for refinement and explained the key articles which' infringement may bring about fines. Section 2.2 explained related works and defined the Model which is used as the input for DPOE Model refinement.

# 3 Current Data Protection Observation Engine (DPOE) Model

The purpose of this section is to review and explain the current DPOE Model (3.1). This section also describes the limitation of the current Model (3.2), stipulates the exclusion and inclusion criteria for DPOE Model refinement (3.2.1) and on that basis, proposes recommendations for the refined DPOE Model (3.2.2).

## 3.1 Current DPOE Model

Tom et al. present a Model representing GDPR entities and their associations (Figure 2) and a Model representing data subject's rights and their associations with GDPR entities (Figure 3) [4].

Figure 2 represents the entities (human or otherwise), actions and artifacts described in the GDPR. Personal data [1, art. 4(1)] is represented with the class `PersonalData` possessing the attribute category `DATA_CATEGORY` to describe the data collected using enumeration. Data processing [1, art. 4(2)] is captured with the class `DataProcessing`. It also covers cross-border processing [1, art.4(23)] of personal data. Attributes `member_states` and `main_establishment` have been used to represent a case where personal data is processed in more than one EU Member State [4]. Technical measures [1, art. 32(1)] are represented with the class `TechnicalMeasures` which is linked to `DataProcessing` via the association `implements`. `TechnicalMeasures` has two attributes `-category` and `-sterotype` which are based on a taxonomy [27] that categorizes privacy-enhancing technologies based on their general privacy goal (also called stereotype). Other key aspects such as consent and different actors have been represented with relevant classes. The roles defined in the GDPR have been generalized under the `Actor` class. As controllers can also be processors, a Boolean attribute `-is_processor` is added to `Controller` class. `Consent` is given for a specific `Purpose` with several attribures (e.g. `freely_given`) that represent conditions under which the consent is valid. `ProcessingLog` artifact is created to meet the requirements of [1, art 30] about maintaining a record of all processing activities [4].

Figure 3 represents rights of the data subjects, associations between them and the classes they impact. For example, Article 16 of the GDPR defines the right of the data subject to have his or her personal data rectified when relevant. This is further linked to the notification obligation placed on the controller if personal data has been rectified as described in Article 19 of the GDPR. Thus, an act of `Rectification` can `trigger` a `Notification` [4].

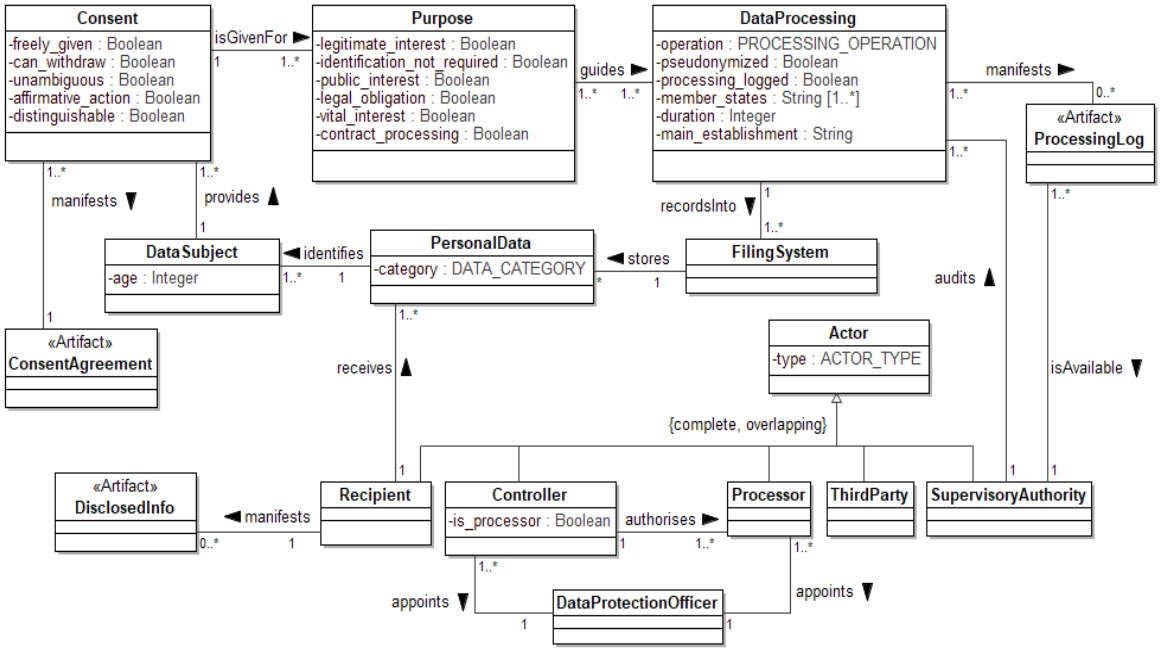


**Figure 2.** GDPR entities and associations (adapted from [4])

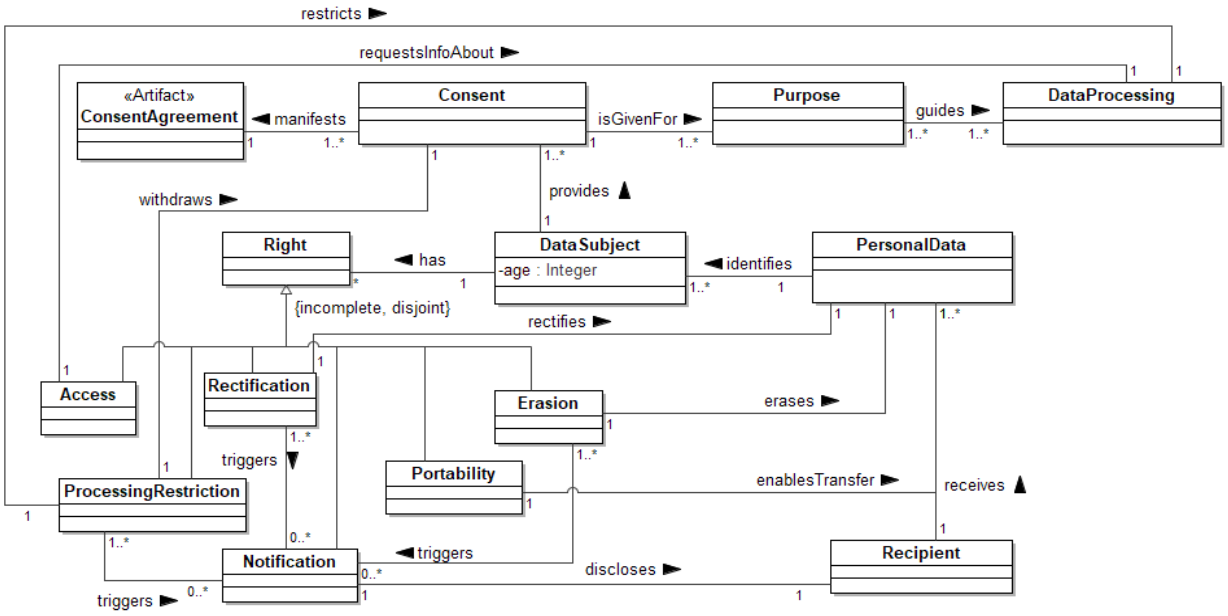


**Figure 3.** Data subject's rights and associations (adapted from [4])

## 3.2 Limitations and Recommendations for Current DPOE Model Refinement

This section describes the limitations of the current DPOE Model (3.2.1) and proposes recommendations for Model refinement based on the inclusion criteria (3.2.2).

### 3.2.1 Limitations of the Current DPOE Model

The current DPOE Model does not cover many GDPR articles described in Articles 83(4) and 83(5) of the GDPR. Hence, avoiding administrative fines under the GDPR is complicated. This is represented by Table 2. Therefore, the legal completeness (i.e. GDPR article coverage) of the Model must be improved to better avoid administrative fines.

**Table 2.** GDPR article coverage of the current DPOE Model. Articles in scope

| **Articles covered by both the current Model and the refined Model** | **Articles not covered by the current Model that are in scope based on the criteria for refinement** |
|---|---|
| 4(1)-4(11), 4(21), 4(23) | 4(12), 4(20), 4(22), 5(1), 5(2), 6(1)-6(4) |
| 7(1)-7(3) | 7(4), 8(1)-8(3), 9(1)-9(4), 10, 11(1)-11(2), 12(1)-12(8), 13(1)-13(4), 14(1)-14(5) |
| 15(1) | 15(2)-15(4) |
| 16 | |
| 17(1), 17(2) | 17(3) |
| 18(1), 18(2) | 18(3) |
| 19 | |
| 20(1), 20(2) | 20(3)-20(4), 21(1)-21(6), 22(1)-22(4), 25(1)-25(3), 26(1)-26(3), 27(1)-27(5) |
| 28(1) | 28(2)-28(10), 29 |
| 30(1), 30(2) | 30(3)-30(5), 31, 32(1)-32(4), 33(1)-33(5), 34(1)-34(4), 35(1)-35(11), 36(1)-36(5) |
| 37(1) | 37(2)-37(7), 38(1)-38(6), 39(1),39(2), 42(1)-42(8), 43(1)-43(9), 44, 45(1)-45(9), 46(1)-(5), 47(1)-(3), 48, 49(1)-49(6) |

Table 2, however, represents the "ideal world" where all the articles based on criteria for refinement are described. Criteria for refinement aim to cover all the articles of the GDPR which might bring about fines under Article 83(4) and 82(5) of the GDPR. Thus, it would be important to capture all the articles described in Table 2 to achieve maximum legal completeness. However, not all articles described in Table 2 provide specific legal requirements for controllers and processors and are fit for modelling. Therefore, criteria for deciding what articles are fit for inclusion and which ones are not is needed. Below, the criteria for excluding (3.2.1.1) and including (3.2.1.2) GDPR articles set out in Table 2 is presented. The criteria are then applied to the articles set out in Table 2. The recommendations for model refinement are presented in 3.2.2.

#### 3.2.1.1 Exclusion Criteria

The exclusion criteria are:

- **Exclusion Rule 1**: to remove from the model all articles set out in Table 2 containing unspecific legal requirements (incl. reasonable effort type of requirements);
- **Exclusion Rule 2**: to remove from the model all articles set out in Table 2 defining requirements for other actors than controller and processor;
- **Exclusion Rule 3**: to remove from the model all articles which define the applicability criteria of articles set out in Table 2 (if-type of requirements). See section 4.2 below; and

- **Exclusion Rule 4**: to remove from the model all articles describing how a legal requirement set out in Table 2 should be applied.

The term "unspecific" must be understood as a vaguely defined requirement which cannot be represented as an activity, association or class in the UML class diagram

Articles meeting the exclusion rules are set out in Appendix I.

#### 3.2.1.2 Inclusion Criteria

The inclusion criteria are:

- **Inclusion Rule 1**: to include to the model all specific legal requirements obliging controllers and processors set out in Table 2;
- **Inclusion Rule 2**: to include to the model requirements that enable the modelling of articles that meet Inclusion Rule 1.

The term "specific" must be understood as a clearly defined requirement which can be represented as an activity, association or class in the UML class diagram.

### 3.2.2 Recommendations for the Current DPOE Model Refinement

Tables 3 and 4 represent the GDPR articles meeting Inclusion Rule 1 and 2. The aim is to give a traceable overview of the modelling proposals made by the author.

**Table 3.** Inclusion of GDPR articles based on Inclusion Rule 1

| Article | How to represent? |
|---|---|
| 5(1) | Class `PrinciplesOfProcessing` with attributes `-lawfulness: Boolean, -purpose_limitation: Boolean, -data_minimisation: Boolean, -accuracy: Boolean, -storage_limitation: Boolean, -integrity_and_confidentiality: Boolean` |
| 5(2) | Association `Controller <<isAccountable>> PrinciplesOfProcessing` |
| 6(1) | Class `LegalGround` with attributes `-consent: Boolean`<br>`-contract: Boolean`<br>`-legal_obligation: Boolean`<br>`-vital_interests: Boolean`<br>`-public_interes: Boolean`<br>`-legitimate_ground: Boolean` |
| 7(2) | Attribute `-distinguishable: Boolean` to class `Consent` |
| 7(3) | Attribute `-can_withdraw: Boolean` to class `Consent` |
| 7(4) | Attribute `-no_bundling: Boolean` to class `Consent` |
| 8(1) | Class `Consent` attribute `-information_society_service_to_child: Boolean` |
| 9(1) | Class `DATA_CATEGORY`. Modified attributes: `-PHILOSOPHICAL_BELIEFS, -TRADE_UNION_MEMBERSHIP, -SEX_LIFE, -SEXUAL_ORIENTATION, -RACIAL_ORIGIN, -ETHNIC` should be changed to `-ETHNIC_ORIGIN` |
| 10 | Class `DATA_CATEGORY`. Modified attribute `-CRIMINAL_RECORD` to `-CRIMINAL_OFFENCE` |
| 12(1) | Attributes `-concise: Boolean, - transparent: Boolean, -intelligible: Boolean, -easily_accessible: Boolean, - clear_and_plain_language: Boolean` of class `Information` |
| 12(2) | `Controller <<enablesExercise>> Right` |
| 12(3) | Attribute `-action_taken_within_30_days: Boolean` of class `Right` |
| 12(4) | Attribute `-informed_datasubject_when_action_not_taken: Boolean` of class `Right` |
| 12(5) | Attribute `-free_of_charge: Boolean` of class `Right` |
| 12(6) | Attribute `-identity_confirmed: Boolean` of class `Right` |
| 13(1) | Class `Information` |
| 14(1) | Class `Information` |
| 15(1) | Class `Access` with attributes `-confirmation_of_processing: Boolean`<br>Specific categories will not be modelled |
| 16 | Class `Rectification` |

| | |
|---|---|
| 17(1) | Class `Erasion`<br>Criteria of applicability will not be modelled |
| 17(2) | Association `Erasion <<triggers>> Notification` |
| 18(1) | Class `ProcessingRestriction`<br>Criteria of applicability described in Articles 18(1)(a)-18(1)(d) will not be modelled |
| 19 | Associations `Rectification <<triggers>> Notification,`<br>`Erasion <<triggers>> Notification,`<br>`ProcessingRestriction <<triggers>>Notification,`<br>`Notification <<discloses>> Recipient` |
| 20(1) | Class `Portability`<br>Criteria of applicability described in Articles 20(1)(a) and (b) will not be modelled |
| 21(1) | Class `Object` with attributes `-legitimate_ground: Boolean, -legal_ground: Boolean` |
| 21(2) | Attribute `-direct_marketing: Boolean` of class `Obejct` |
| 22(1) | Class `NotToBeSubjectToAutomatedDecision` |
| 25(1) | Class `TechnicalMeasures` and class `OrganisationalMeasures` |
| 25(2) | Class `TechnicalMeasures` and class `OrganisationalMeasures` |
| 27(1) | Class `Representative`, generalization of class `Actor` |
| 28(3) | Attribute `-has_mandate: Boolean` to `Processor` |
| 28(10) | Attribute `-is_controller: Boolean` to class `Processor` |
| 30(1) | Class `<<Artifact>>ProcessingLog` with attributes `-name_and_contact_details: Boolean, -purposes_of_processing: Boolean, -categories_of_data_subjects: Boolean, -categories_of_personal_data: Boolean, -categories_of_recipients: Boolean, -third_countries_data_is_transferred: Boolean, -data_retention_periods: Boolean, -technical_and_organisational_measures_applied: Boolean` |
| 30(2) | Class `<<Artifact>>ProcessingLog` with attributes `-name_and_contact_details: Boolean, -purposes_of_processing: Boolean, -categories_of_data_subjects: Boolean, -categories_of_personal_data: Boolean, -categories_of_recipients: Boolean, -third_countries_data_is_transferred: Boolean, -data_retention_periods: Boolean, -technical_and_organisational_measures_applied: Boolean` |
| 30(4) | Association `ProcessingLog <<isAvailable>> SupervisoryAuthority` |
| 31 | Association `Controller <<coOperates>> SupervisoryAuthority` |
| 32(1) | Classes `TechnicalMeasures` and `OrganisationalMeasures` |
| 35(7) | Attributes `-description_of_processing_activities: Boolean, -necessity_and_proportionality_assessment: Boolean, -measures_mitigating_risks: Boolean` of class `<<Artifact>>DataProtectionImpactAssessment` |
| 37(1) | Association `Controller <<appoints>> DataProtectionOfficer`<br>`Processor <<appoints>> DataProtectionOfficer`<br>Applicability criteria of Articles 37(1)(a)-(c) will not be modelled |
| 37(7) | Attribute `-contact_details_published: Boolean` to class `DataProtectionOfficer` |

**Table 4.** Inclusion of GDPR articles based on Inclusion Rule 2

| Article | How to represent? |
|---|---|
| 4(1) | Class `PersonalData` with attributes `-related_to_identifiable_natural_person: Boolean, -data_category: DATA_CATEGORY` |
| 4(2) | Class `DataProcessing` with attributes `- operation: PROCESSING_OPERATION, - pseudonymised: Boolean, - processing_logged: Boolean, - member_states: String [1..*], - duration: Integer, -main_establishment: Boolean,- impact_assessment: Boolean, -data_breach: Boolean, -third_country: Boolean` |
| 4(3) | Class `ProcessingRestriction` |
| 4(4) | Attribute `-PROFILING` of class `PROCESSING_OPERATION` |
| 4(5) | Attribute `-pseudonymised: Boolean` of class `DataProcessing` |
| 4(6) | Class `FilingSystem` |
| 4(7) | Class `Controller` |
| 4(8) | Class `Processor` |

| | |
|---|---|
| 4(9) | Class `Recipient` |
| 4(10) | Class `ThirdParty` |
| 4(11) | Class `Consent` with attributes `-unambiguous: Boolean, -affirmitive_action: Boolean, -distinguishable: Boolean, -freely_given: Boolean, -specific: Boolean, -informed: Boolean, -no_bundling: Boolean` |
| 4(22) | Class `SupervisoryAuthority`<br>It is assumed that "supervisory authority concerned" is meant |
| 26(1) | Attribute `+is_joint_controller: Boolean` of class `Controller` |

### 3.3 Summary

This section identified several articles that are not covered by the current Model (see Table 2) giving rise to the assumption that the legal completeness (i.e. GDPR article coverage) of the current Model could be improved in light of avoiding administrative fines under the GDPR. This section also proposed modelling recommendations based on the Inclusion Rules (Tables 3 and 4). These recommendations form a base for the refined Model is represented in section 4.1.

# 4 Refined Data Protection Observation Engine Model

The purpose of this section is to propose a refined DPOE Model (4.1) together with the applicability criteria (4.2). This section also compares the current Model to the refined Model in terms of GDPR article coverage and presents results thereof (4.3).

## 4.1 Refined DPOE Model

Figures 4 and 5 illustrate the refined DPOE Model. The refined Model is created based on the recommendations set out in 3.2.2.

Figure 4 presents the refined Model of entities and associations. It includes the class `LegalGround` to present that `DataProcessing` must have a legal ground (whether consent or other). Consent is seen as one separate class (`Consent`) that manifests one of the legal grounds. The `LegalGround`, in turn, guides `DataProcessing` by setting the limits to processing personal data. New classes related to `DataProcessing` (linked with association `<<has>>` are: `LegalGroundDataTransfer`, `LegalGroundSpecialCategory` and `<<Artifact>>DataProtectionImpactAssessment`. These classes represent GDPR articles 45-59, 9(2) and 35-36 respectively. The class `DataProcessing` which could be said to be the center of the universe in the refined Model, includes three new attributes (`-impact_assessment: Boolean`, `-data_breach: Boolean` and `-third_country: Boolean`) to accommodate these new classes. Also, the refined DPOE Model includes a new class `OrganisationalMeasures` which the `Controller` needs to apply to `DataProcessing`. The refined Model includes the obligation to make a data breach notification in case of a data breach (class `DataBreachNotification`). The refined Model now includes data processing principles and the principle of accountability (`Controller<<isAccountable>>PrinciplesOfProcessing`) to cover Article 5 of the GDPR. In terms of actors, the refined Model includes `DataSubject` to the list of actors. Also, class `Representative` is included as an actor to meet the requirements of Article 27 of the GDPR. This means that there is a complete list of actors represented in the refined DPOE Model. Also, the class `<<Artifact>>ProcessingLog` has now attributes describing the content requirements for the records of processing in accordance with Article 30(1) and 30(2) of the GDPR.

Figure 5 presents the refined Model of data subjects' rights and associations. It includes three new rights – `Information`, `Object` and `NotToBeSubjectToAutomatedDecision`. These rights cover GDPR articles 13-14, 21 and 22 respectively. The addition of these rights means that all the data subjects rights set out in the GDPR are now covered in the Model. The class `Rights` has three new attributes covering GDPR articles 12(3)-12(6) - `-action_taken_within_30_days: Boolean`, `-informed_datasubject_when_action_not_taken: Boolean`, `-free_of_charge: Boolean` and `-identity_confirmed: Boolean`. Also, the refined Model incorporates `Controller` to the `Model` who is the key actor as it is responsible for the exercise of the data subjects' rights (`Controller <<enablesExercise>>Right`).

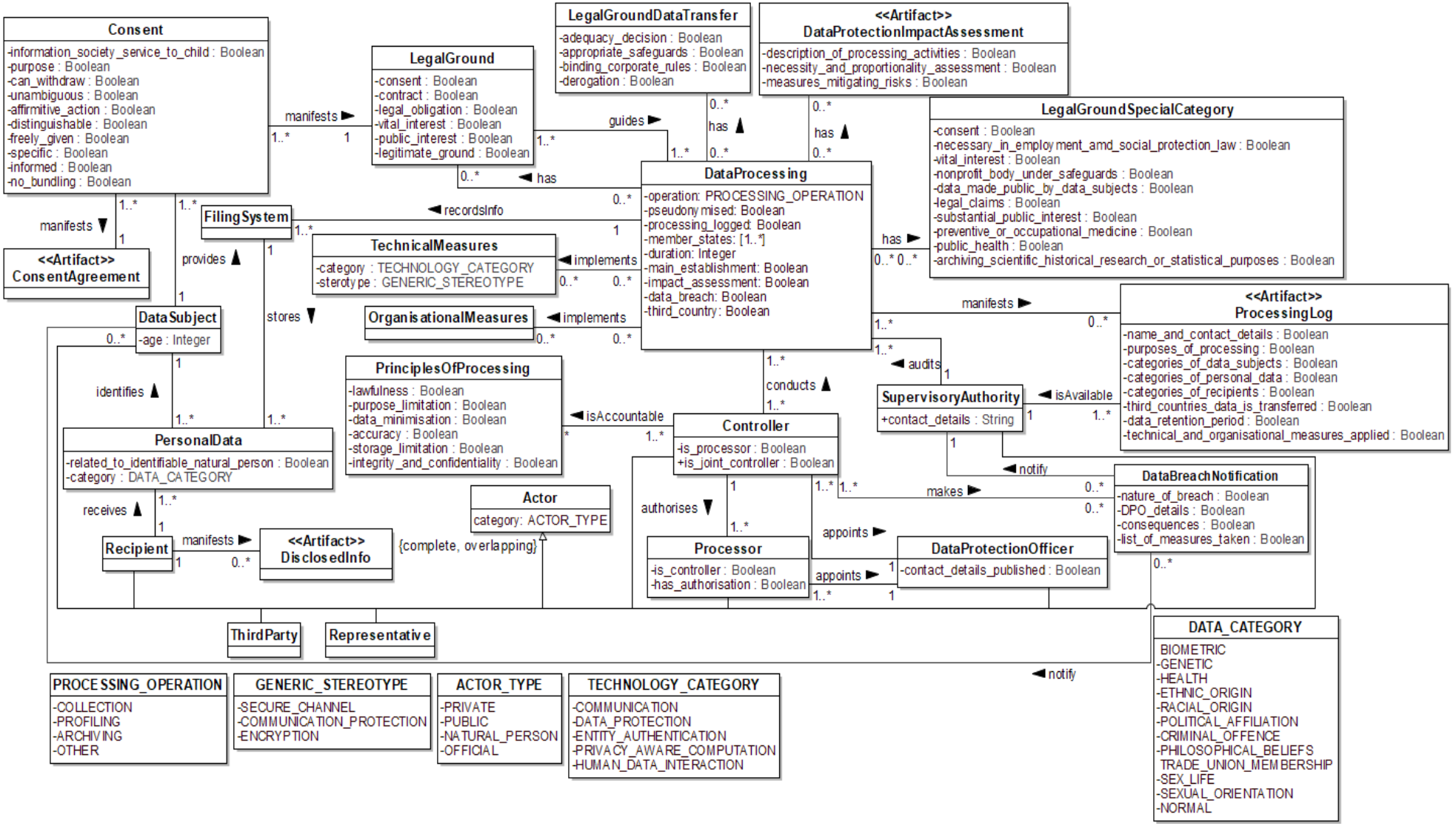


**Figure 4.** Refined DPOE Model: GDPR entities and associations

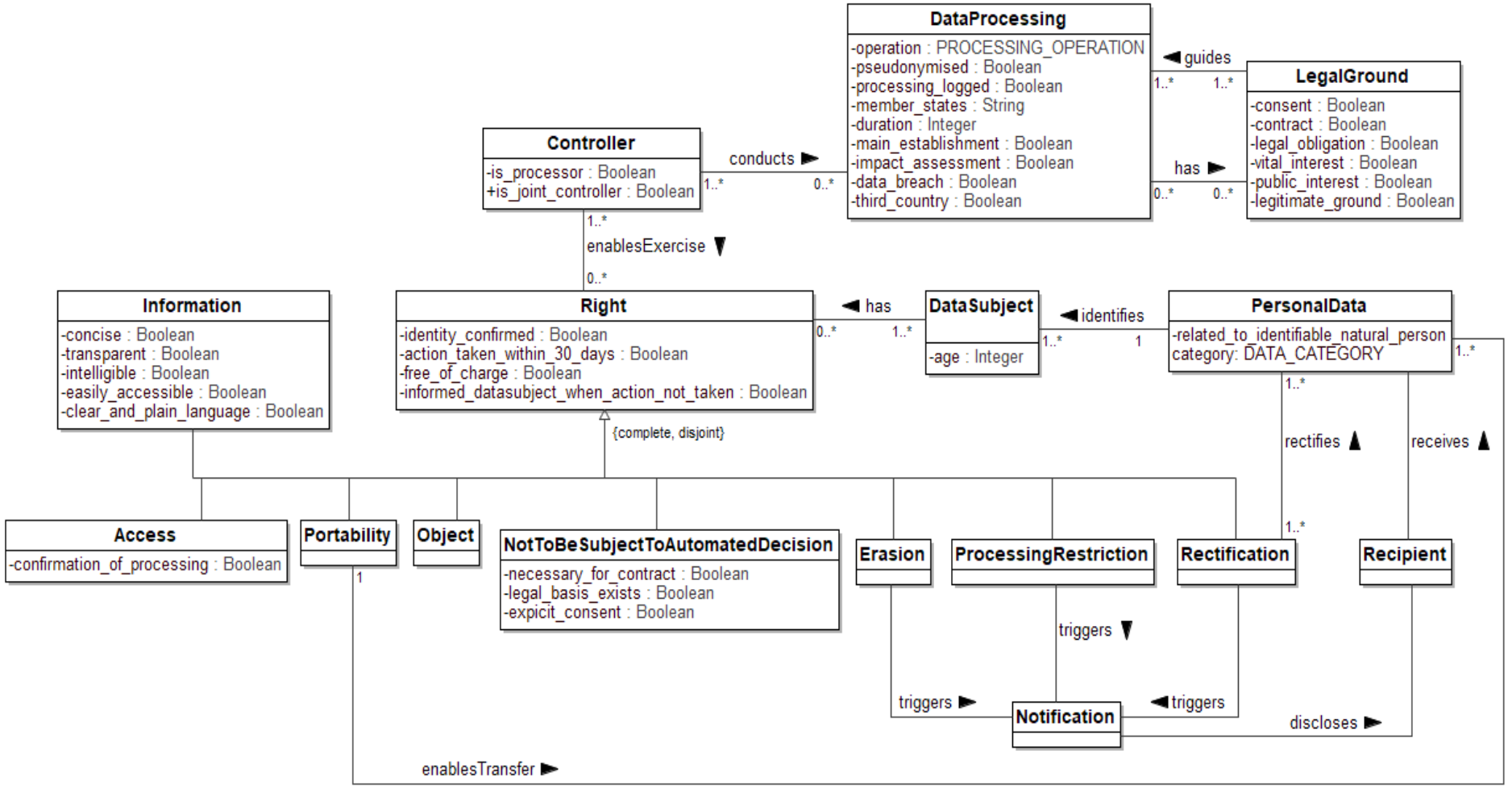


**Figure 5.** Refined DPOE Model: Data subject's rights and associations

## 4.2 Applicability Criteria

Certain occurrences of the GDPR were excluded from the DPOE Model because they met Exclusion Rule 3. The UML modelling language does not support the modelling of if-type requirements (these were seen to meet Exclusion Rule 3). That said, several requirements that were excluded under this rule are important requirements that require modelling as they form important requirements under the criteria for refinement. Therefore, the author has selected key articles meeting Exclusion Rule 3 and modelled the applicability criteria in BPMN. The key applicability criteria could be described as special cases of data processing. These are:

1) Conducting a DPIA or prior consultation with the supervisory authority (Articles 35 and 36 of the GDPR; see 4.2.1);
2) Processing of special categories of data on a legal basis (Article 9(2) of the GDPR; see 4.2.2);
3) Transferring personal data to a third country (Articles 45(1), 46(1), 46(2), 46(3), 47(1) and 49(1) of the GDPR; see 4.2.3); and
4) Making a data breach notification in case of a data breach (Articles 33 and 34 of the GDPR; see 4.2.4).

Negative ends (e.g. “Processing prohibited”, “No”, “Processing not permitted”) are the flows or scenarios which raise a “red flag” in terms of GDPR compliance in the context of a given BPMN model. Positive end-events (e.g. “Processing may begin”, “Data transfer permitted”) mean that there is no (potential) GDPR violation. Data objects describe what is the input (arrow pointing to task) and output (arrow pointing from task) of each task are to enable linking the tasks with elements of the refined Model.

### 4.2.1 Data Protection Impact Assessment and Prior Consultation

In certain scenarios under the GDPR, the controller must conduct a DPIA prior or consult with a supervisory authority. If the application of the applicability criteria set out in Figure 6 renders the result that a DPIA must be concluded, the attribute `-impact_assessment: Boolean` of class `DataProcessing` must have value 1. In such a scenario, the instantiation of the Model must include class `<<Artifact>>>DataProtectionImpactAssessment`.

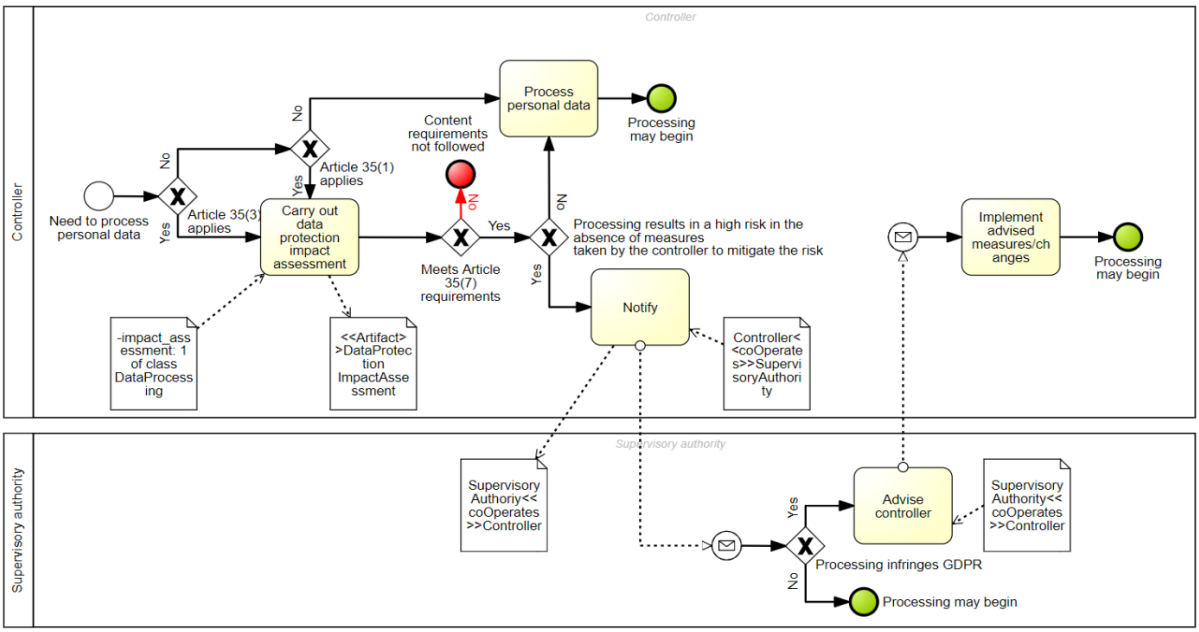


**Figure 6.** Conducting a data protection impact assessment and consulting with the supervisory authority

**Business process model description:** If a need to initiate a new type of processing activity exists (class `DataProcessing` attribute `-impact_assessment: Boolean = 1`), the controller needs to verify whether a DPIA needs to be conducted. Article 35(3) of the GDPR stipulates three grounds when a DPIA is compulsory. If such a ground exists, the controller needs to conduct a DPIA. See attributes of class `<<Artifact>>DataProtectionImpactAssessment` in Figure 4 to see what the compulsory elements are. If Article 35(3) of the GDPR does not a apply, the controller needs to verify whether it still needs to conduct a DPIA under Article 35(1) of the GDPR. If Article 35(1) of the GDPR applies, the controller must conduct a DPIA. If not, the controller has verified that no DPIA needs to be conducted in the current case and the processing of personal data may begin.

If the controller needs to conduct a DPIA, it needs to comply with some content requirements as set out in Article 35(7) of the GDPR. If not applied, the controller is in breach of the GDPR. More information may be presented in the DPIA, but not less than described in Article 35(7) of the GDPR.

If, as a result of the DPIA, the controller finds that the processing results in a high risk in the absence of measures taken by the controller to mitigate the risk, controller must notify the supervisory authority. If such a high risk does not exist, the controller may proceed with processing personal data as it has met the GDPR requirements.

Once the notification has reached the supervisory authority, the supervisory authority must verify whether the processing infringes the GDPR. If not, the controller may proceed to process personal data as the GDPR requirements are complied with. If yes, the supervisory authority must advise the controller how to be compliant in the specific case. In such a case, the controller needs to implement the advised measures to start processing personal data.

**Table 5.** Coverage of Articles 35 and 36 of the GDPR in Figure 6

| Article | Comment | How is it represented in the BPMN model |
|---|---|---|
| 35(3) | Data protection impact assessment must be conducted if Article 35(3) applies | Gateway `Article 35(3) applies` XOR `Yes` |
| 35(1) | Data protection impact assessment must also be conducted if certain type of processing may bring about a high risk to the rights and freedoms of natural persons | Gateway `Article 35(1) applies` XOR `Yes` |
| 36(1) | If processing results in a high risk in the absence of measures taken by the controller to mitigate the risk, controller must notify the supervisory authority | Task `Notify Message` to Supervisory authority |
| 36(2) | If the supervisory authority finds that the GDPR is infringed, it shall advise the controller | Gateway `Processing infringes GDPR` XOR `Yes` Task `Advise controller Message` to Controller |

### 4.2.2 Processing Special Categories of Personal Data

The applicability criteria set out in Figure 7 must be used when attribute `-category: DATA_CATEGORY` of class `PersonalData` has value ≠ `NORMAL` (i.e. the value is either `-BIOMETRIC, -GENETIC, -HEALTH, -ETHNIC_ORIGIN, -RACIAL_ORIGIN, - POLITICAL-AFFILIATION, -GENDER, -CRIMINAL_OFFENCE, - PHILOSOPHICAL_BELIEFS, -TRADE_UNION_MEMBERSHIP, -SEX_LIFE` or `-SEXUAL_ORIENTATION`). In such an occurrence, the instantiation of the Model must include class `LegalGroundSpecialCategory` with the respective attribute representing Articles 9(2)(a) to 9(2)(j) of the GDPR marked with value 1. If there is no legal ground (i.e. all attribute value in class `LegalGroundSpecialCategory` have value 0), the processing of special categories of data is not permitted.

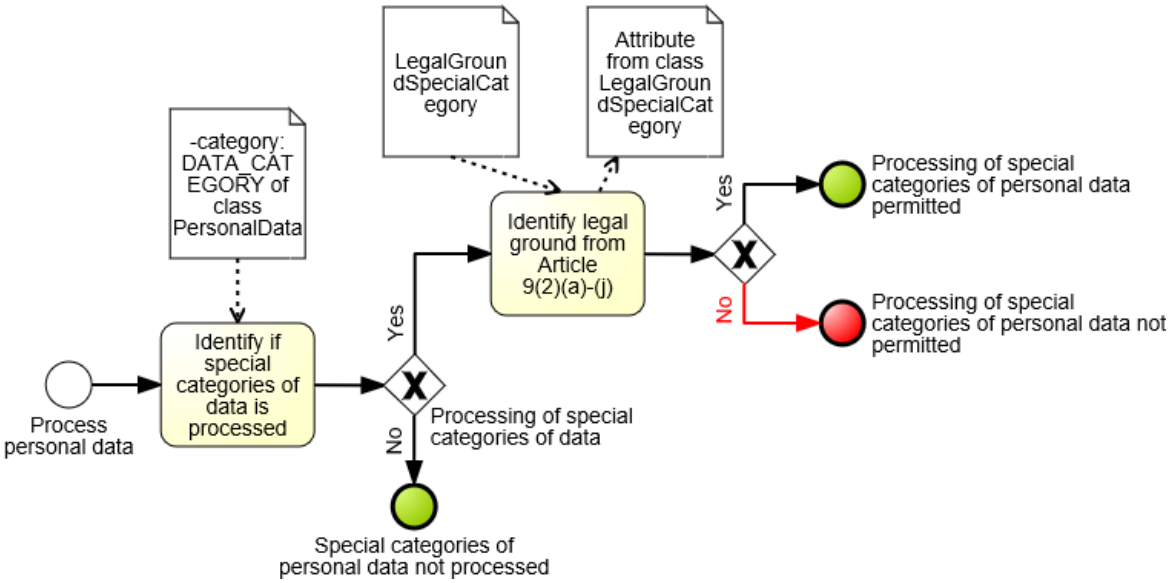


**Figure 7.** Processing of special categories of data in accordance with Article 9(2) of the GDPR

**Business model description:** If special categories of data are processed, the controller needs to identify a legal ground for this. As Article 9(2) of the GDPR stipulates other legal grounds for the processing of special categories of data as it does to the processing of personal data, the controller needs to verify that it has a legal ground as stated in Article 9(2) of the GDPR. If no special categories of data are processed, then this model does not apply, and personal data processing may take place provided that a legal ground exists as presented in the class `LegalGround` of the refined Model.

If special categories of data are processed, then the controller needs to have a legal ground from Article 9(2)(a)-(j) (represented as class `LegalGroundSpecialCategory` in the refined Model). Identification requires marking one of the attributes (`-consent: Boolean, -necessary_in_employment_and_social_security_and_social_protection_law: Boolean, -vital_interest: Boolean, -nonprofit_body_under_safeguards: Boolean, -data_made_public_by_data_subject: Boolean, -legal_claims: Boolean, -substantial_public_interest: Boolean, -preventive_or_occupational_medicine: Boolean, -public_health: Boolean, -archiving_scientific_historical_research_or_statistical purposes: Boolean`) of class `LegalGroundSpecialCategory` to 1 if such a ground exists. If not, then processing of special categories of personal data is not permitted as there is no legal ground for this. If any of the attributes can be marked as 1, then processing of special categories of personal data is permitted. If none of the attributes can be marked as 1, the controller does not have a legal ground. If it nevertheless processes the special categories of data, it is in breach of Article 83(5) of the GDPR.

**Table 6.** Coverage of Article 9(2) of the GDPR in Figure 7

| Article | Comment | How is it represented in the BPMN model |
|---|---|---|
| 9(2) | Processing of special categories of personal data is permitted if there is a legal ground specified in Article 9(2)(a)-9(2)(j) | Gateway `Processing of special categories of data` XOR<br>Task `Identify legal ground from Article 9(2)(a)-(j)` |

### 4.2.3 Transfer of Personal Data to Third Countries

Transfer of personal data to third countries requires a legal basis. If there is a need to transfer personal data to a third country (i.e. attribute `-third_country: Boolean` of class

DataProcessing has value 1), the controller needs to identify whether there is a legal ground for such transfer. In such an occurrence, the instantiation of the Model must include class LegalGroundDataTransfer. The legality of the data transfer must be verified based on the applicability criteria set in Figure 8. If as a result of the applicability criteria the controller reaches an end "data transfer permitted", the respective attribute of the class LegalGroundDataTransfer must have value 1. If there is no legal basis for a data transfer, the attribute values of class LegalGroundDataTransfer have value 0.

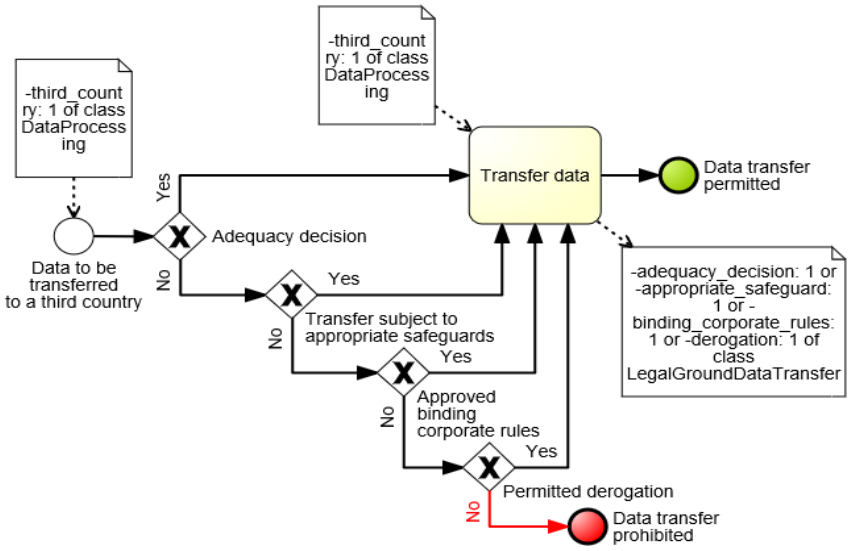


**Figure 8.** Data transfer to third countries under Articles 45, 46, 47 and 49 of the GDPR

**Business model description:** If a need to transfer data to third country arises (class DataProcessing attribute -third_country: Boolean = 1), the controller must verify whether it has a legal ground described in Chapter V of the GDPR for such a transfer (represented as class LegalGroundDataTransfer in the refined Model). The first legal ground is a European Commission's adequacy decision (attribute -adequacy_decision: Boolean of class LegalGroundDataTransfer). If the third country is subject to an adequacy decision, the controller may transfer the data to the third country and the data transfer is legal in terms of the GDPR. If there is no adequacy decision, the controller needs to assess whether the transfer could take place on the appropriate safeguards (attribute -appropriate_safeguards: Boolean of class LegalGroundDataTransfer). If yes, the transfer is compliant with the GDPR. If not, the controller must assess whether the base of such a data transfer could be binding corporate rules (attribute -binding_corporate_rules: Boolean of class LegalGroundDataTransfer). If such approved corporate rules exist, the data transfer is legal. If not, the controller must assess whether the data transfer could have a specific derogation described in Article 49(1) of the GDPR (attribute -derogation: Boolean of class LegalGroundDataTransfer). If yes, the transfer is legal. If not, there is no ground for the controller to transfer personal data to a third country and the data transfer is prohibited. If the controller still transfers data to a third country, it is an infringement of the GDPR.

**Table 7.** Coverage of Articles 45(1), 46(1), 46(3), 47(1) and 49(1) of the GDPR in Figure 8

| Article | Comment | How is it represented in the BPMN model |
|---|---|---|
| 45(1) | Transfer of personal data to a third country is permitted if the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organization in question ensures an adequate level of protection | Gateway `Adequacy decision` XOR |
| 46(1) | Transfer of personal data to a third country is permitted if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. If there is are appropriate safeguards listed in Article 46(2), no authorization from the supervisory authority is required | Gateway `Transfer subject to appropriate safeguards` XOR |
| 47(1) | Transfer of personal data to a third country is permitted if supervisory authority has approved binding corporate rules | Gateway `Approved binding corporate rules` XOR |
| 49(1) | Transfer of personal data to a third country is permitted if a specific derogation exists in Article 49(1)(a)-49(1)(g) for data transfer | Gateway `Permitted derogation` XOR |

### 4.2.4 Data Breach Notification

When a data breach occurs, the controller is obliged to notify either the supervisory authority or in certain cases, the data subjects. If the attribute `-data_breach: Boolean` of class `DataProcessing has` value 1, the controller needs to identify whether it needs to notify the supervisory authority or also the data subjects. If a data breach notification must be made under the applicability criteria set out in Figures 9 or 10, the instantiation of the Model must include class `DataBreachNotification` in that case. Figure 9 describes the process of deciding whether the supervisory authority needs to be notified.

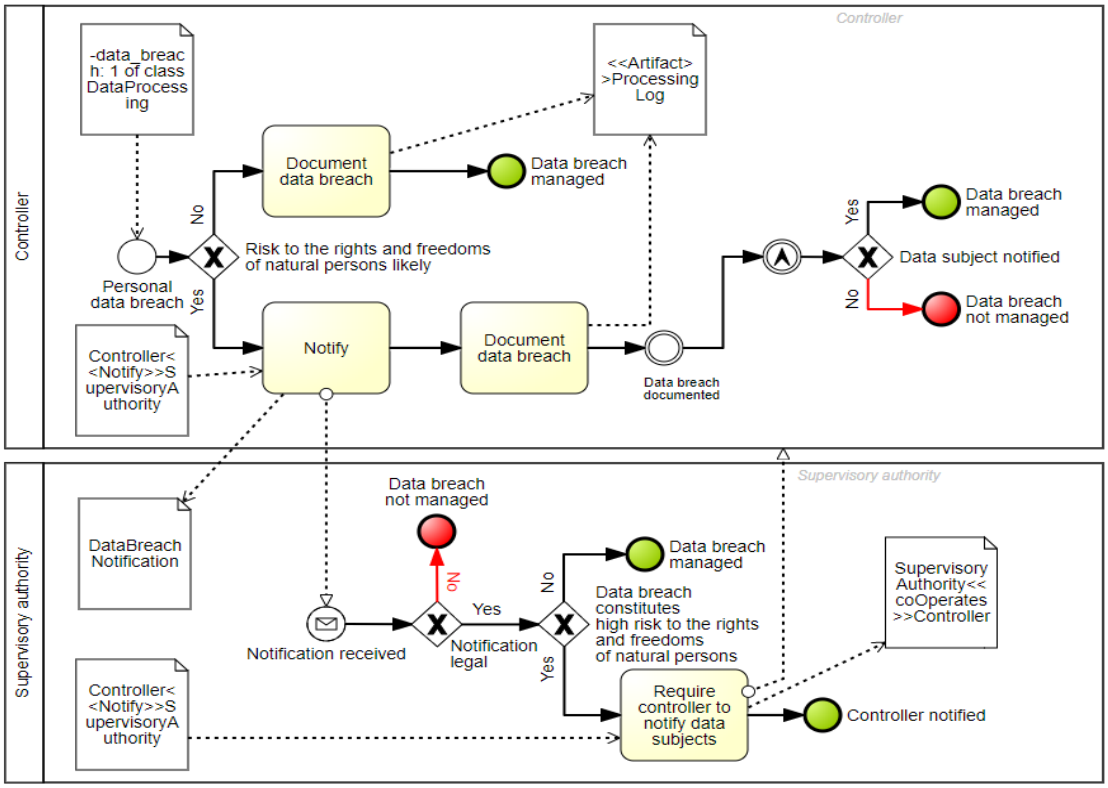


**Figure 9.** Data breach notification based on Article 33 of the GDPR

**Business model description:** In case of a personal data breach (class `DataProcessing` attribute `-data_breach: Boolean = 1`), the notification of the supervisory authority depends first on the fact whether the breach constitutes a likely risk to the rights and freedoms of data subjects. If no, then the controller is obliged to document the relevant aspects concerning the data breach [1, art. 35(3)] and the data breach is managed in compliance with the GDPR. If, however, a likely risk arises, the controller is obliged to notify the supervisory authority (represented as association `DataBreachNotification<<Notify>>SupervisoryAuthority` in the refined Model). The controller is still obliged to document the details of the breach. If this is done, the process reaches to an intermediate end which is restarted if an escalation event by the supervisory authority reaches the controller.

The notification must be made in accordance with the GDPR. If the supervisory authority receives the notification, it will verify whether the data breach constitutes a high risk to the rights and freedoms of the data subjects. If not, the data breach is managed by the controller in compliance with the GDPR. If the supervisory authority finds that the data breach constitutes high risk to data subjects, it requires the controller to notify data subjects about the breach. If the notification reaches the controller, the controller is obliged to notify the data subjects in accordance with Article 34 of the GDPR. If this is done, the data breach is managed in compliance with the GDPR by the controller. If not done, controller is in breach of the GDPR.

**Table 8.** Coverage of Article 33 of the GDPR in Figure 9

| **Article** | **Comment** | **How is it represented in the BPMN model** |
|---|---|---|
| 33(1) | Personal data breach must be communicated to the supervisory authority if there is a risk to the rights and freedoms of natural persons | Gateway `Risk to the rights and freedoms of natural persons` XOR `Yes`<br><br>Annotation `Must be made within 72 hours after data breach` |
| 33(3) | The notification communicated to the supervisory authority must contain information set out in Article 33(3) of the GDPR | Gateway `Notification legal` |
| 33(5) | Data breach details must be documented | Task `Document data breach` |
| 34(4) | Supervisory authority may require the controller to notify data subjects about the data breach in accordance with Article 34 of the GDPR | Gateway `Data breach constitutes high risk to the rights and freedoms of natural persons` XOR `Yes`<br>Task `Require controller to notify data subjects`<br>`Message to controller`<br>Task `of controller to Notify data subjects` |

Figure 10 represents the process for deciding whether data subjects must be notified after a data breach.

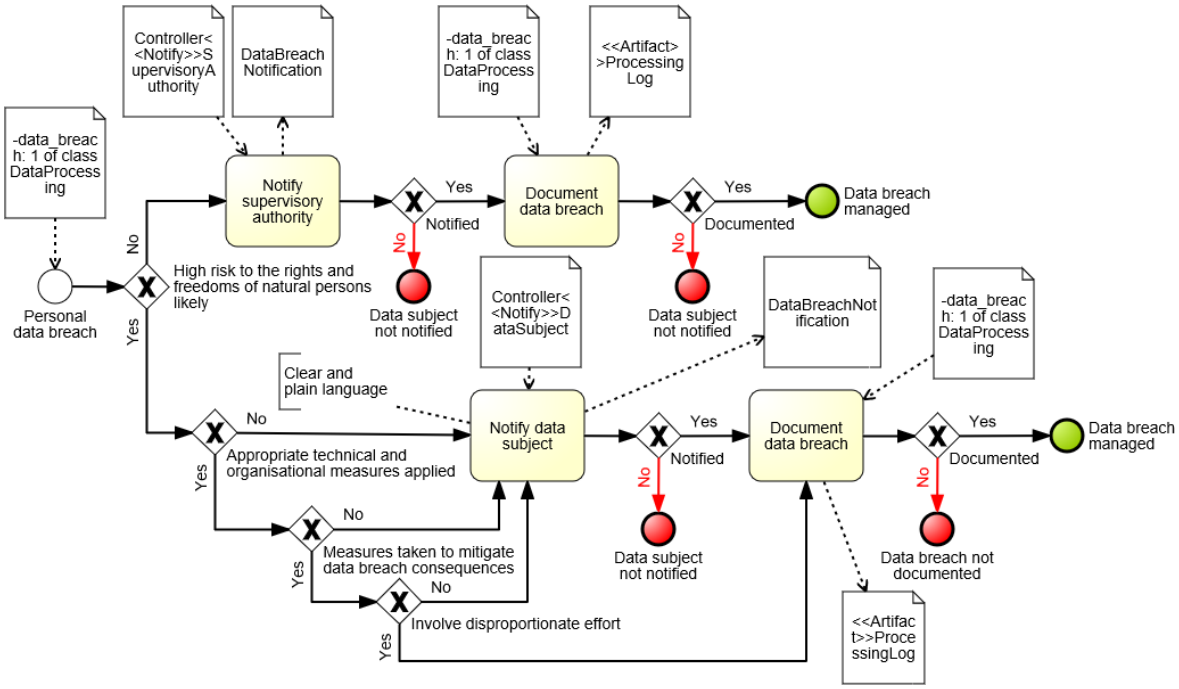


**Figure 10.** Data breach notification based on Article 34 of the GDPR

**Business model description:** If a high risk to the data subjects arises due to the data breach (class `DataProcessing` attribute `-data_breach: Boolean = 1`), the controller may be obliged to notify the data subjects instead of the supervisory authority. If a breach occurs, the controller needs to first verify if high risk is present. If no, the process described in Figure 9 is essentially triggered (represented as tasks `Notify supervisory authority`, `Document data breach`). If, however, high risk is present, the GDPR presents several conditions that enable the controller not to notify the data subject. Firstly, the controller must assess whether appropriate technical and organizational measures were applied. If yes, then it must assess whether it took measures to mitigate data breach consequences. If yes, then it must assess whether notification of data subjects affected would be a disproportionate effort. If yes, then controller must document the data breach details together with the assessment why the notification was not needed. If this is done, the data breach causing high risk to the data subjects is managed in accordance with the GDPR. However, if any of these assessments render the answer “no”, the controller must notify the data subjects affected (represented as association `DataBreachNotification<<Notify>>DataSubject` in the refined Model). If not notified, the controller is in breach of the GDPR. If notification is made and the data breach is documented in accordance with the GDPR, the controller has managed the data breach in accordance with the GDPR.

**Table 9.** Coverage of Article 34 of the GDPR in Figure 10

| Article | Comment | How is it represented in the BPMN model |
|---|---|---|
| 34(1) | Personal data breach must be communicated to the data subject if there is high a risk to the rights and freedoms of natural persons | Gateway `High risk to the rights and freedoms of natural persons` XOR `Yes` |
| 34(2) | Communication to the data subject must be in clear and plain language | Annotation `In clear and plain language` for task `Notify data subject` |
| 34(3) | Personal data breach must be communicated to the data subject only if: a) no appropriate technical and organizational measures are applied; b) no measures were taken to mitigate the consequences of data breach; and c) communication would not involve disproportionate effort | Gateways `Appropriate technical and organisational measures applied`, `Measures taken to mitigate data breach consequences`, `Involve disproportionate effort` |

## 4.3 Comparison of the GDPR Article Coverage by the Current and Refined Models

As a result of the application of the inclusion and exclusion criteria (3.2.1.1 and 3.2.1.2), the legal completeness (i.e. GDPR article coverage) of the current and refined Models can be compared. The aim of the refinement process was to include GDPR articles that meet the criteria for refinement and meet the inclusion rules. Table 10 represents the GDPR articles covered by the current DPOE Model and the refined Model.

**Table 10.** Comparison of the legal completeness (i.e. GDPR article coverage) of the current and refined Models

| Current Model | Refined Model |
|---|---|
| 4(1) | 4(1) |
| 4(2) | 4(2) |
| 4(3) | 4(3) |
| 4(4) | 4(4) |
| 4(5) | 4(5) |
| 4(6) | 4(6) |
| 4(7) | 4(7) |
| 4(8) | 4(8) |
| 4(9) | 4(9) |
| 4(10) | 4(10) |
| 4(11) | 4(11) |
| 4(21) | **X** |
| **X** | 4(22) |
| 4(23) | 4(23) |
| **X** | 5(1) |
| **X** | 5(2) |
| **X** | 6(1) |
| 7(1) | **X** |
| 7(2) | 7(2) |
| 7(3) | 7(3) |

| Current Model | Refined Model |
|---|---|
| **X** | 7(4) |
| **X** | 8(1) |
| **X** | 8(2) |
| **X** | 8(3) |
| **X** | 9(1) |
| **X** | 9(2)* |
| **X** | 10 |
| **X** | 11(1) |
| **X** | 11(2) |
| **X** | 12(1) |
| **X** | 12(2) |
| **X** | 12(3) |
| **X** | 12(4) |
| **X** | 12(5) |
| **X** | 12(6) |
| **X** | 13(1) |
| **X** | 14(1) |
| 15(1) | 15(1) |
| 16 | 16 |
| **X** | 17(1) |

| Current Model | Refined Model |
|---|---|
| **X** | 17(2) |
| **X** | 18(1) |
| 18(2) | **X** |
| 19 | 19 |
| 20(1) | 20(1) |
| 20(2) | **X** |
| **X** | 21(1) |
| **X** | 21(2) |
| **X** | 22(1) |
| **X** | 25(1) |
| **X** | 25(2) |
| **X** | 26(1) |
| **X** | 27(1) |
| 28(1) | **X** |
| **X** | 28(3) |
| **X** | 28(10) |
| 30(1) | 30(1) |
| 30(2) | 30(2) |
| **X** | 30(4) |
| **X** | 30(5) |

| Current Model | Refined Model |
|---|---|
| **X** | 31 |
| **X** | 32(1) |
| **X** | 33(1)* |
| **X** | 33(3)* |
| **X** | 33(5)* |
| **X** | 34(1) |
| **X** | 34(2)* |
| **X** | 34(4)* |
| **X** | 35(1)* |
| **X** | 35(3)* |
| **X** | 35(7) |
| **X** | 36(1)* |
| **X** | 36(2)* |
| 37(1) | 37(1) |
| **X** | 37(7) |
| **X** | 44* |
| **X** | 45(1)* |
| **X** | 46(1)* |
| **X** | 47(1)* |
| **X** | 49(1)* |

* - applicability criteria modelled in BPMN (see section 4.2)

Although the current Model was aimed to give a general visual overview of the associations between the key entities set out in the GDPR, the aim of refined Model was to include articles from the perspective of administrative fines. Both Models, however, have the same goal to help organization in gaining a better overview of the GDPR and achieve compliance. Therefore, the two Models can be compared in terms of GDPR article coverage.

Out of 191 articles in scope (see Table 2), the refined Model covers 75 GDPR articles (≈39 %) while the current Model covers 26 articles (≈ 14%). Thus, the refined Model covers 49 more GDPR articles (25% more than the current Model). The current Model covers five GDPR articles which are not covered in the refined Model.

### 4.4 Summary

Section 4 presented the refined Model (4.1) together with the applicability criteria (4.2). As a result, the current and refined Models could be compared in terms of legal completeness (4.3). It was concluded that the refined Model covers 49 GDPR articles more than the current DPOE Model.

# 5 Application of the Current and Refined DPOE Models to Business Process Model

The purpose of this section is to apply both the current and refined Models to an actual business process model (5.2) in order to compare the instantiations of both Models and identify how each Model helps to avoid fines under the GDPR (5.4). The method for comparing the two Models is set out in 5.1. Section 5.3 presents the aspects that threat the validity of the results presented in 5.4.

## 5.1 Method and Business Process Model Description

In this section, the method for compliance review based on both Models is described (5.1.1) and the description of the business process model and the extraction rules are provided (5.1.2).

### 5.1.1 Method for Comparing DPOE Models

The thesis will use the iterative method described by Sing [26]. The high-level steps of this method are:

1) **Extract as-is compliance model**: the actual business process model in BPMN is taken as the input together with additional input from the user to instantiate the business process model in UML. In the current thesis, this will be done manually. However, it could be developed into a semi-automatic or even an automatic method in the future.
2) **Compare two meta-models**: once the as-is model is instantiated, it can be compared to a previously defined GDPR meta-model.
3) **Define compliance issues**: based on found differences of two models, this step gives a binary answer to the question whether the extracted compliance model is GDPR-compliant or not and give a detailed descriptions of business process incompliances.
4) **Change business process model**: this is an optional step that could be taken if the previous step renders unsatisfactory results.

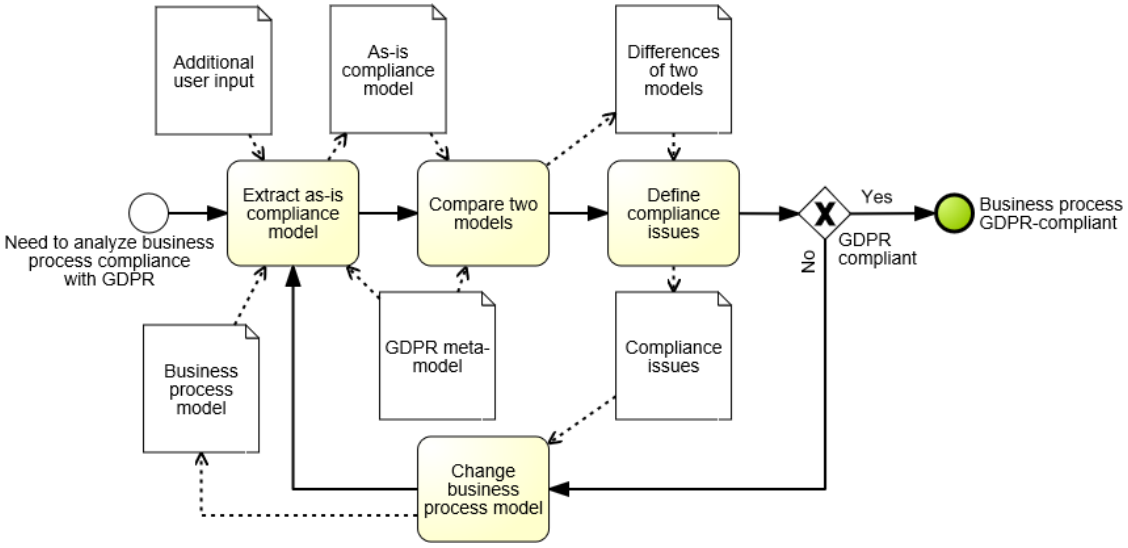


**Figure 11.** Method for comparing Models (adapted from [26])

### 5.1.2 Business Process Model Description and Extraction Rules

The business process used is the case of ÕIS2 (*Haridustasemete ülese õppeinfosüsteem 2*) used by Sing [26] with modifications. ÕIS2 is developed by Fujitsu Estonia AS and is procured by Estonian Educational Technology Foundation (HITSA). ÕIS2 is funded by European Structural and Investment Funds. ÕIS2 will serve as a study information system for Estonian colleges, vocational schools and professional higher education institutions [26]. As ÕIS2 was adopted after the entering into force of the GDPR [28] the need to conduct a DPIA must also be analyzed.

In [26], ÕIS2 registration was presented as a business process based on consent. This assumption is challenged here. ÕIS (ÕIS2 is an update of ÕIS) is the central study information system where all the information is shared, where students register for courses and where grades are inserted by university staff, a student has no real choice not to use ÕIS. Therefore, one of the preconditions for consent – freely given – is not fulfilled. For example, the Study Regulations of the University of Tartu [29] stipulate that "the official environment for exchanging information related to the organization of study of the university is the Study Information System" (*i.e. ÕIS*) [29]. There are several references in the Study Regulations that indicate that a user must do certain activities in ÕIS and cannot to them any other way [29, IV.4.61, IV.4.62, IV.5.63, V.3.105.2, IX.1.162]. Moreover, the Privacy Policy stipulates that the purposes for processing information in ÕIS (i.e. first name, family name, ID code, date of birth, origin, citizenship and contact details) "arise from University of Tartu Act and Universities Act and are necessary for the purposes of identifying the student, organizing teaching and studies, creating a user account for the student in the university's computer system, and issuing academic documents" [30]. Therefore, the business process model used by Sing in [26] requires modifications as the example business process presented does not rely on consent as a legal basis, but a legal act.

The modifications are as follows (see Figure 12):

1) Task `Ask for consent` changed to `Ask for information` in pool `ÕIS2`; and
2) Task `Provide consent` changed to `Provide information` in pool `User`.

The reason is that the right to process personal information and the right to ask for additional information does not come from consent but from a legal act. This, in turn, means that modifications to the extraction rules set out in [26] must be made as well.

Extraction rules for extracting an as-is compliance model:

- **Extraction Rule 1**: Actors
- **Extraction Rule 2**: Personal data and data subject
- **Extraction Rule**: Filing system
- **Extraction Rule 4**: Processing activities
- **Extraction Rule 5**: Records of processing
- **Extraction Rule 6**: Legal ground
- **Extraction Rule 7**: Measures
- **Extraction Rule 8**: Disclosure
- **Extraction Rule 9:** Principles of processing
- **Extraction Rule 10:** Data subject rights

The running example business process model used to compare the current and refined Models is described in Figure 12.

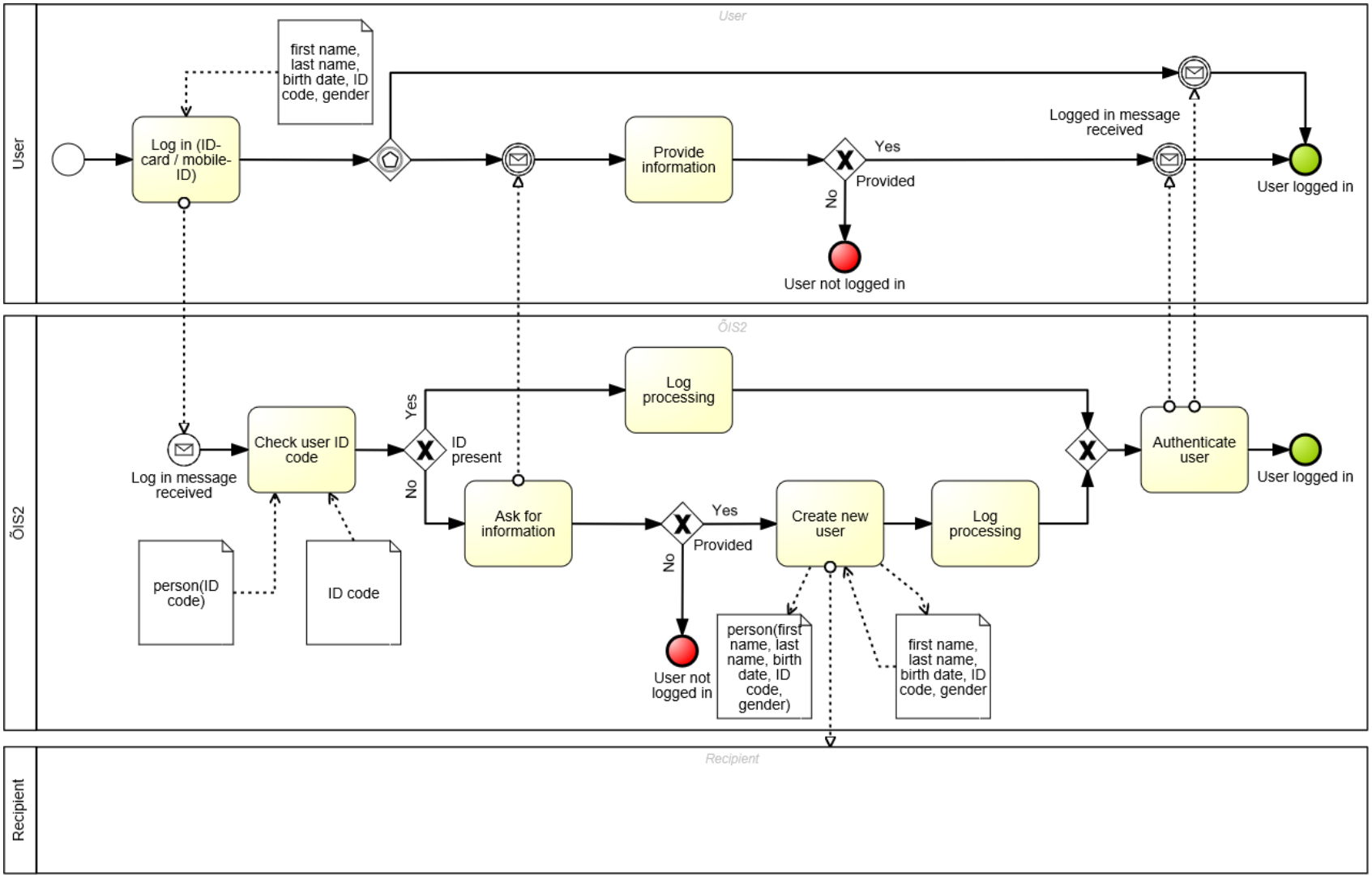


**Figure 12.** User login process model (running example)

## 5.2 Application of the Current and Refined DPOE Models to the Business Process Model

In this section, the feasibility of the refined DPOE Model compared to the current DPOE Model is ascertained (SUBQ3).

### 5.2.1 Extraction Rule 1: Actors

Extraction of the actors is a manual process as the business process model does not contain information about the roles and actors.

#### 5.2.1.1 Current Model

The current Model includes four main actors besides supervisory authority (controller, processor, recipient (see 5.2.8), third party). From 5.1.2 the following information can be extracted: HITSA is the controller while Fujitsu Estonia AS is the entity acting on behalf of HITSA while developing and maintaining ÕIS2 (i.e. it is a processor).

Each actor has a type in the current Model. In case of HITSA, it is `PUBLIC`. For Fujitsu Estonia AS, it is `PRIVATE`. In the current Model, the attribute `-is_processor` is used which means that the `Controller` can also be a `Processor`.

#### 5.2.1.1 Refined Model

In the refined Model, there are six actors besides supervisory authority (controller, processor, recipient (see 5.2.8), third party, data subject (see 5.2.2) and representative). The amount of information available only enables extracting information about the controller and the processor. However, there are extra attributes that are added compared to the current Model. Firstly, attribute `+is_joint_controller` of the class `Controller` to reflect whether there are other entities who define the purposes and means of processing [1, art. 26]. Secondly, class `Processor` has now attributes `-is_controller` and `-has_authorisation` to reflect GDPR articles 28(10) and 28(3) of the GDPR. As there is no such information, the Boolean values will be 0 for these attributes.

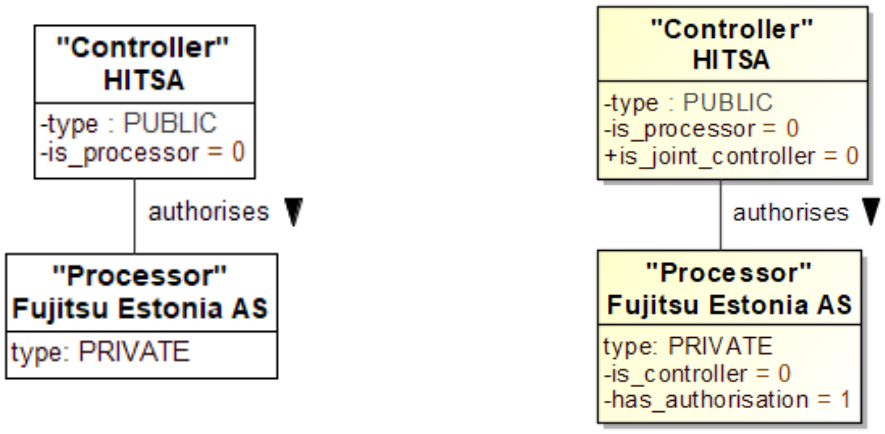


**Figure 13.** Comparison of application of Extraction Rule 1 for current Model (left, white) and refined Model (right, yellow)

### 5.2.2 Extraction Rule 2: Personal Data and Data Subjects

`PersonalData` is depicted as data objects and could be read automatically from the business process model. The data category (class `DATA_CATEGORY`) requires input from the controller.

DataSubject could either be represented as a pool or lane in which case this information can be extracted from the business process model automatically. In case of several pools or lanes, the FilingSystem (also represented as a pool or lane) needs to be identified first and then DataSubject can be identified later. This could be a semi-automatic activity.

#### 5.2.2.1 Current Model

Personal data has several sub-rules to follow:

1) PersonalData is depicted in the process model as data objects. Instances of used data objects are depicted as list of string separated by a comma. Each label is a separate piece of PersonalData.

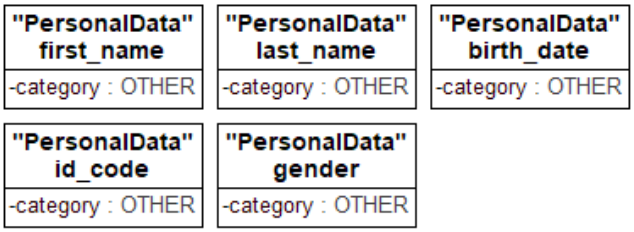


**Figure 14.** Example of Extraction Rule 2 sub-rule 1 (current)

2) Data object can identify several DataSubject. In this case, data subjects have to be separated with line change and DataSubject label, and all PersonalData labels of a single DataSubject have to be contained in parenthesizes (e.g. person(id code)).
3) In case of Extraction Rule 2 sub-rule 1, there is no annotated DataSubject in the data object but information about the DataSubject can be extracted from the pool or lanes of the BPMN model. However, as there are usually more than one pool or lane and reading pool or lane is also how FilingSystem is detected in Extraction Rule 3 (5.2.3), reading the Extraction Rule 3 must take place before extracting Extrction Rule 2 sub-rule 3 [26].
   The class PersonalData has attribute -category: DATA-CATEGORY. In the current Model, the -category is OTHER (NORMAL in the refined Model) for all PersonalData instances.
   The class DataSubject has attribute -age: Integer. There is no information about the age of the Student.

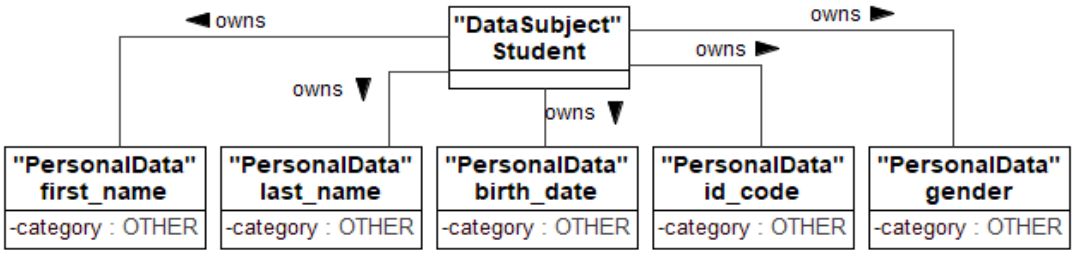


**Figure 15.** Example of Extraction Rule 2 sub-rule 3 (current)

4) PersonalData can be contained in databases. To represent this, a data object with property "set" has been used in the process model (e.g. person(first name, last name, birth date, id code, gender)). With this property, different tables can be represented simultaneously in one data object.

#### 5.2.2.2 Refined Model

Application of the `PersonalData` and `DataSubject` classes in the refined Model renders similar results than for the current Model. Compared to the current Model, the refined Model adds one attribute which is probably assumed in the current Model for `PersonalData`, but not explicitly stated: `-related_to_identifiable_natura_person: Boolean`.

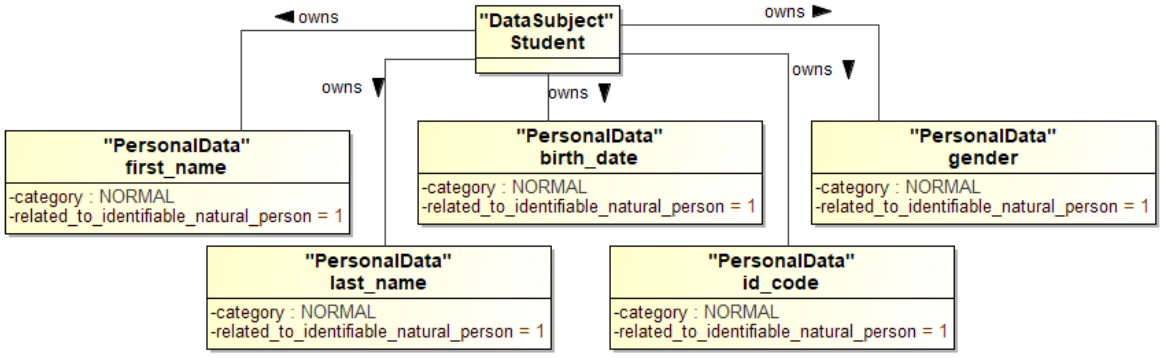


**Figure 16.** Example Extraction Rule 2 sub-rule (refined)

### 5.2.3 Extraction Rule 3: Filing System

`FilingSystem` is represented as a pool or lane in the business process model. This information can be extracted automatically from the business process model.

#### 5.2.3.1 Current Model

`FilingSystem` is represented as a pool or lane. For the ease of reading the model, `PersonalData` instances `first_name`, `last_name` and `id_code` is used instead of all five `PersonalData` instances.

#### 5.2.3.2 Refined Model

As the `FilingSystem` instantiation of the refined Model is like the current Model except for the added attribute for class `PersonalData` discussed in 5.2.2, only the results of the refined Model will be presented.

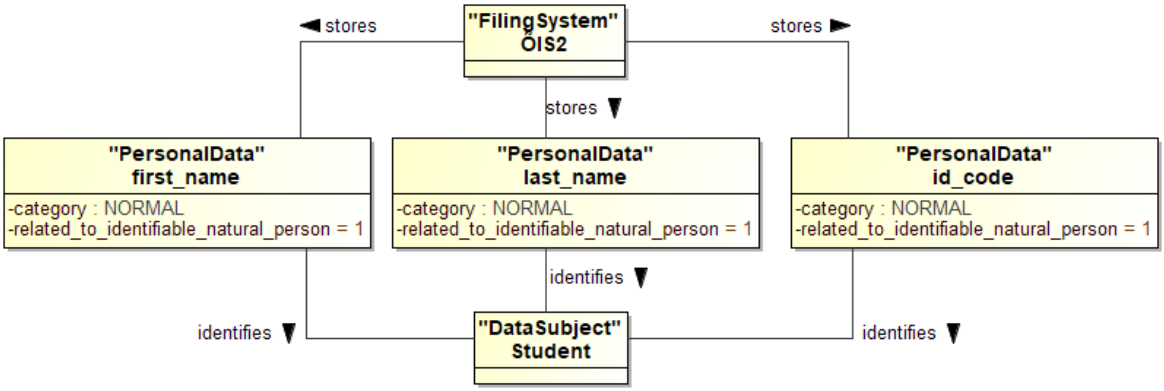


**Figure 17.** Example of Extraction Rule 3 (refined)

### 5.2.4 Extraction Rule 4: Processing Activities

`DataProcessing` activities are represented as tasks of the business process model with ingoing and outgoing connections to data objects in pools that represent the `FilingSystem`.

Prior to `DataProcessing`, the controller might be obliged to conduct a DPIA. Thus, before new type of `DataProcessing` is commenced, the business process model set out 3.2.2.1 needs to be followed manually.

#### 5.2.4.1 Current Model

In the current Model, `DataProcessing` has the following attributes: `-operation: PROCESSING_OPERATION`, `-pseudonymized: Boolean`, `-processing_logged: Boolean`, `-member_states: String [1..*]`, `-duration: Integer` and `-main_establishment: String`.

Using the information available, attributes `-operation`, `-pseudonymized` and `-processing_logged` can be filled. Figure 18 below uses one processing activity () to exemplify how a `DataProcessing` instance is represented in the current Model (Create new user). From the incoming data objects in the business process model, only three are used (first name, last name, id code). Attribute `-processing_logged` value is set to 1 as the business process model includes an activity "Log processing".

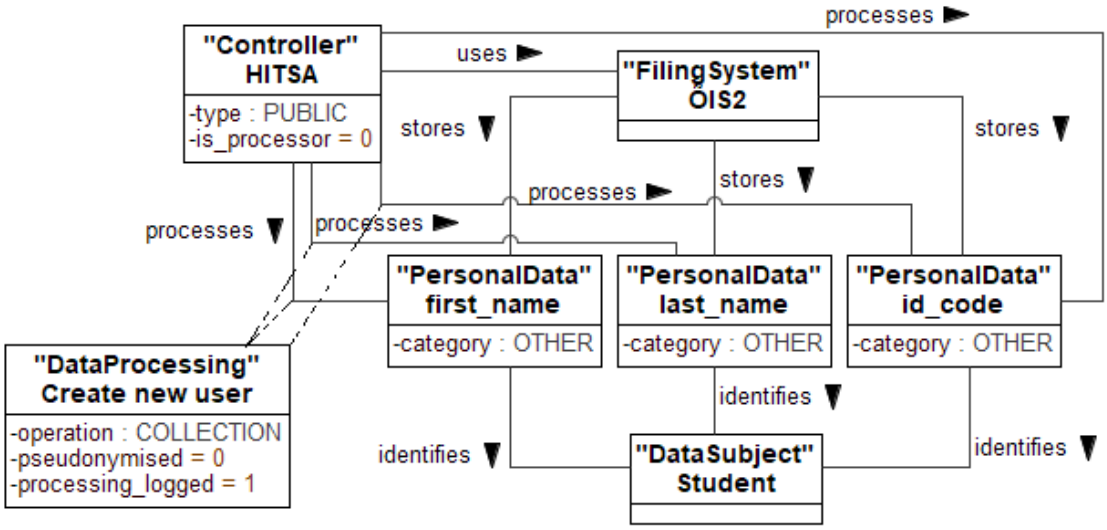


**Figure 18.** Example of Extraction Rule 4 (current)

As it was stated in 5.1.2, ÕIS2 was adopted after the adoption of the GDPR. This means that the controller must assess under Article 35 of the GDPR whether a DPIA must be conducted. However, the current Model does not represent or refer to such an obligation. Therefore, the assessment whether a DPIA should be conducted or not is not represented by the current Model.

#### 5.2.4.1 Refined Model

In the refined Model, class `DataProcessing` has three new attributes: `-impact_assessment: Boolean`, `-third_country: Boolean` and `-data_breach: Boolean`. Although there is no information about transferring data to a third country and about a data breach, the refined Model addresses the obligation of the controller to assess whether a DPIA needs to be conducted. The information in 5.1.2 triggers the applicability criteria set out in 4.2.1.

To apply the DPIA process model set out in 4.2.1 to the running example, the result is as follows: Article 35(3) of the GDPR does not apply (Gateway `Article 35(3) applies` XOR `No`). Then, assessment of Article 35(1) needs to take place. As the processing of ÕIS2 compared to ÕIS is most probably not different in nature and scope and would not, therefore, result in a high risk to the rights and obligations of the data subjects, there is no need conduct a DPIA. However, there is not enough information on this available and input about the

actual nature, scope and technologies used would be required from the controller. In this case, it is assumed that no DPIA needs to be conducted (Gateway `Article 35(1) applies` XOR `No`). This means the processing may begin and the value of the attribute - `impact_assessment` is 0.

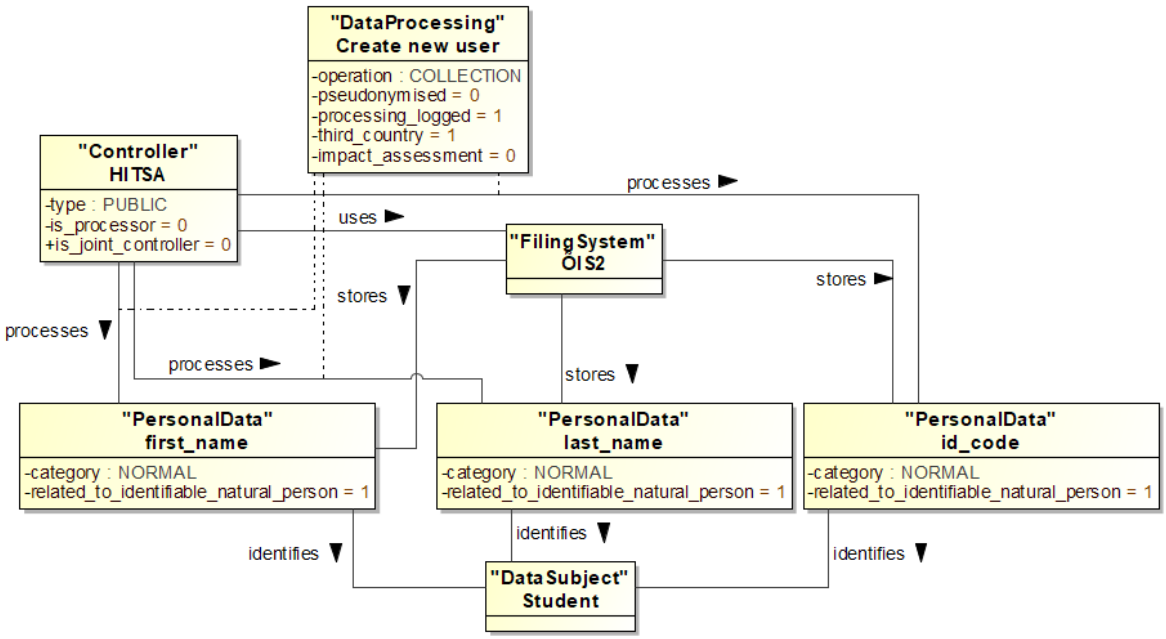


**Figure 19.** Example of Extraction Rule 4 (refined)

### 5.2.5 Extraction Rule 5: Records of Processing

`ProcessingLog` may be represented as a task (e.g. “Log processing” or “Log”). If represented as a such task, this information may be extracted automatically. However, not all business process models might represent this information as a task and thus, it may also be a semi-automatic activity or manual activity depending on the business process model.

#### 5.2.5.1 Current Model

Recording processing activities is mandated under [1, art. 30]. It is one of the measures under which controller can demonstrate compliance. In the running example, it is represented as an activity “Log processing” which takes place after processing activities. Processing activity is undertaken after the activities “Create new user” and “Check user ID code”.

#### 5.2.5.2 Refined Model

The refined Model for representing logging of processing is similar except to the extent attributes are covered by different classes described above. Thus, only the results rendered by the extraction of the refined Model is represented below with the example of one `PersonalData` instance (`id_code`).

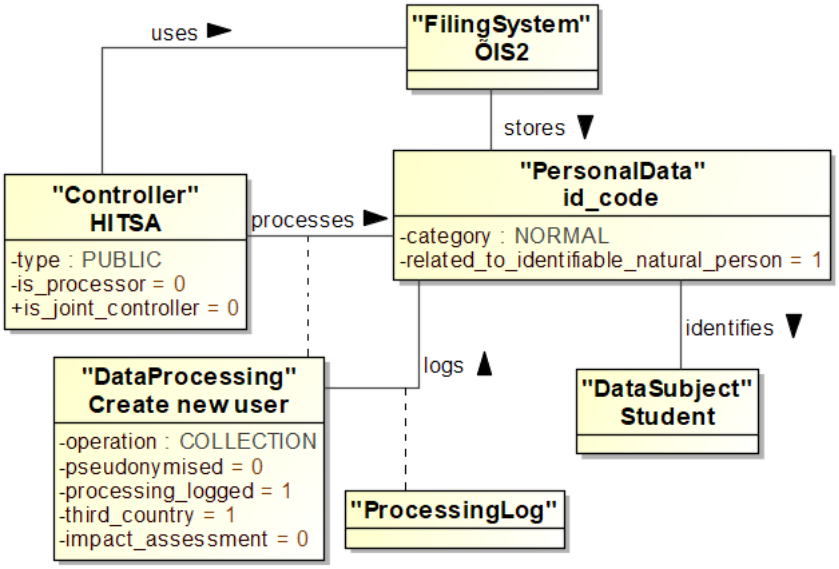


**Figure 20.** Example of Extraction Rule 5 (refined)

### 5.2.6 Extraction Rule 6: Legal Ground

Legal ground needs input from the controller and cannot be read from the business process model. Thus, it is a manual activity.

#### 5.2.6.1 Current Model

Since the legal ground for processing login information in the business process model is law [1, art. 6(1)(e)], the current Model does not address this situation specifically. The current Model focuses on consent (class `Consent`) which is given for a purpose (class `Purpose`). The attributes of class `Purpose` include legal grounds stipulated in [1, art. 6(1)(b)- 6(1)(f)]. However, from a legal perspective, attribute `-public_interest: Boolean` cannot be an attribute of `Purpose` as purpose is something the controller defines. Tom et al. state that the current Model should be read in a fashion that if any of the attributes of `Purpose` are 1, then the `DataProcessing` does not need consent as a legal basis [4]. Currently, the value of attribute `-public_interest` is 1. The actual purpose of an activity “Create new user” is to enable the use of ÕIS2 by a legitimate user.

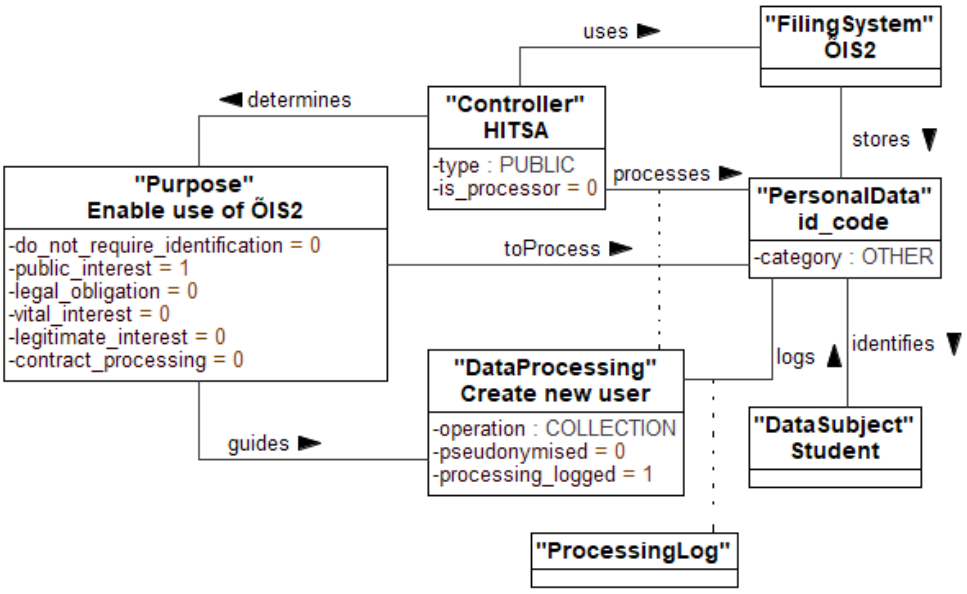


**Figure 21.** Example of Extraction Rule 6 (current)

#### 5.2.6.2 Refined Model

In the refined Model, `DataProcessing` is linked with class `LegalGround` with the association `<<has>>`. Also, an association `Controller<<conducts>>DataProcessing` exists which is aligned with the logic of data processing. `LegalGround`, in turn, guides `DataProcessing` as it sets limits and describes the purpose (`LegalGround<<guides>>DataProcessing`). In the refined Model, data processing must have a legal ground and the legal grounds set out in [1, art. 6(1)] are stipulated as attributes of the class `LegalGround`. As we identified that the legal ground for processing is a legal act, the attribute `-public_interest` has value 1.

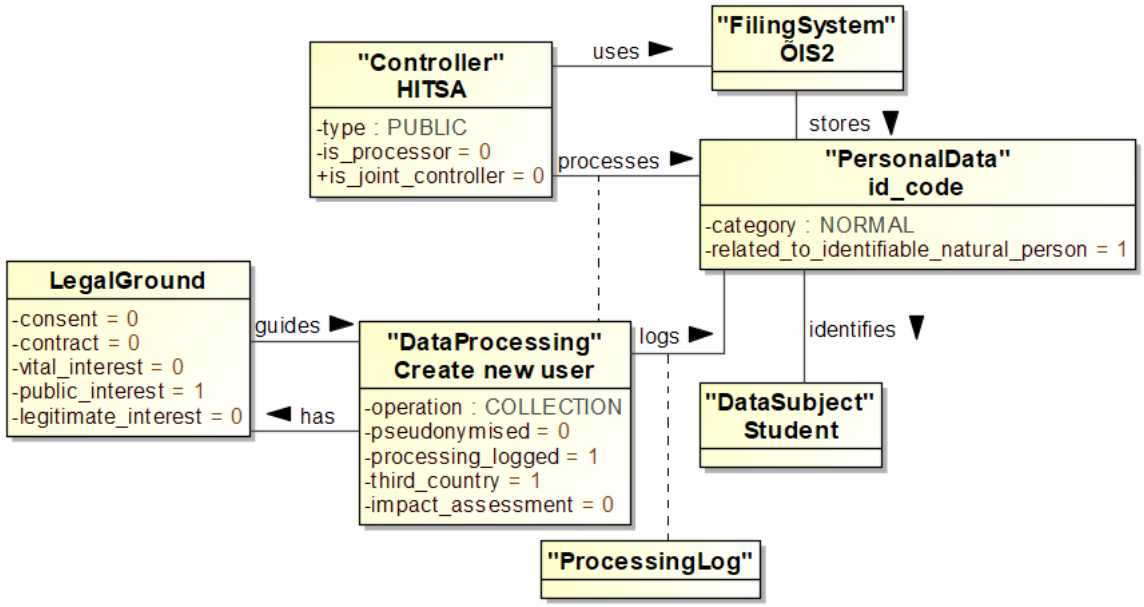


**Figure 22.** Example of Extraction Rule 6 (refined)

### 5.2.7 Extraction Rule 7: Measures

The business process model does not include information about the technical and organizational measures implemented to `DataProcessing` to guarantee data confidentiality, integrity

and availability [1, art. 32]. Therefore, this input is required from the controller making it a manual activity.

#### 5.2.7.1 Current Model

The current Model includes association `DataProcessing<<implements>>TechnicalMeasures`. Class `TechnicalMeasures` has attributes `-category: TECHNOLOGY_CATEGORY` and `-stereotype: GENERIC_STEREOTYPE`. As there is no information about the technical measures implemented, the attributes are not extracted. The current Model does not include a class addressing organizational measures.

#### 5.2.7.2 Refined Model

Compared to the current Model, the refined Model includes class `OrganisationalMeasures`. This makes the Model complete in terms of measures set out in [1, art. 32]. Although there is no information available about the content of the measures, it is assumed that the measures exist and are therefore, included in the Model.

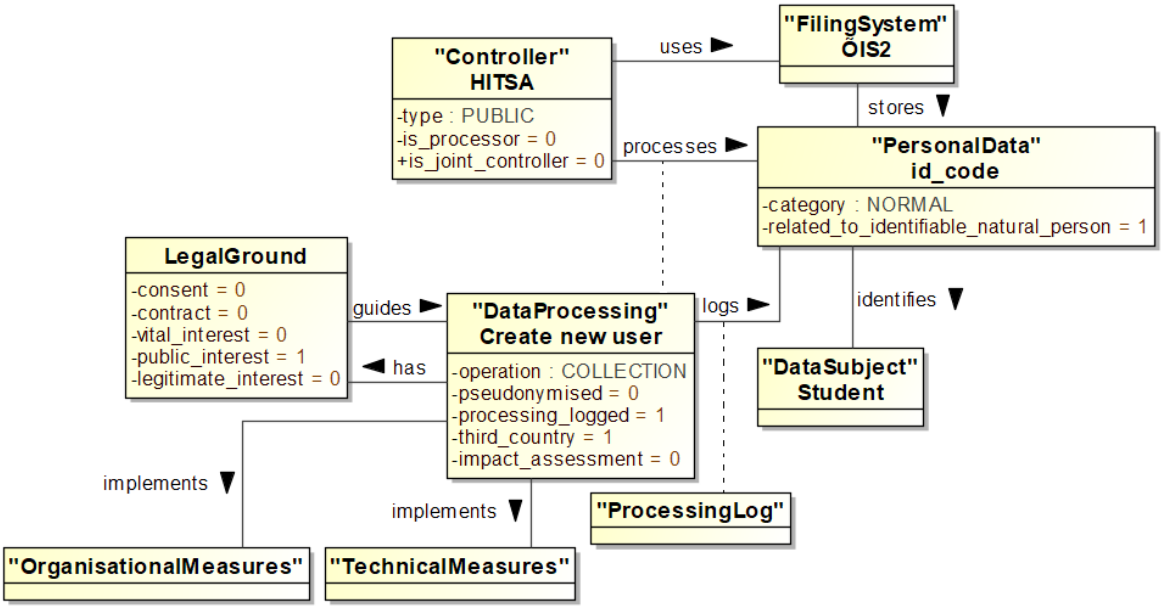


**Figure 23.** Example of Extraction Rule 7 (refined)

### 5.2.8 Extraction Rule 8: Disclosure

`Recipient` is represented as a message flow leaving the pool of `FilingSystem` and not going to the direction of `DataSubject`. The pool or lane where the message flow is directed is the `Recipient`. This information can be extracted from the business process model automatically.

Manual input is required to identify whether the `Recipient` is inside or outside of the EU. If outside the EU, the data transfer needs a legal base and the applicability criteria set out in 4.2.3 is triggered.

#### 5.2.8.1 Current Model

In the example, “Create new user” activity has a message flow to pool “Recipient”. This represents the act of disclosing personal data to a recipient. The information disclosed to the `Recipient` is “information about a new user”.

The information disclosed is represented as class `<<Artifact>>DisclosedInfo` in the current Model.

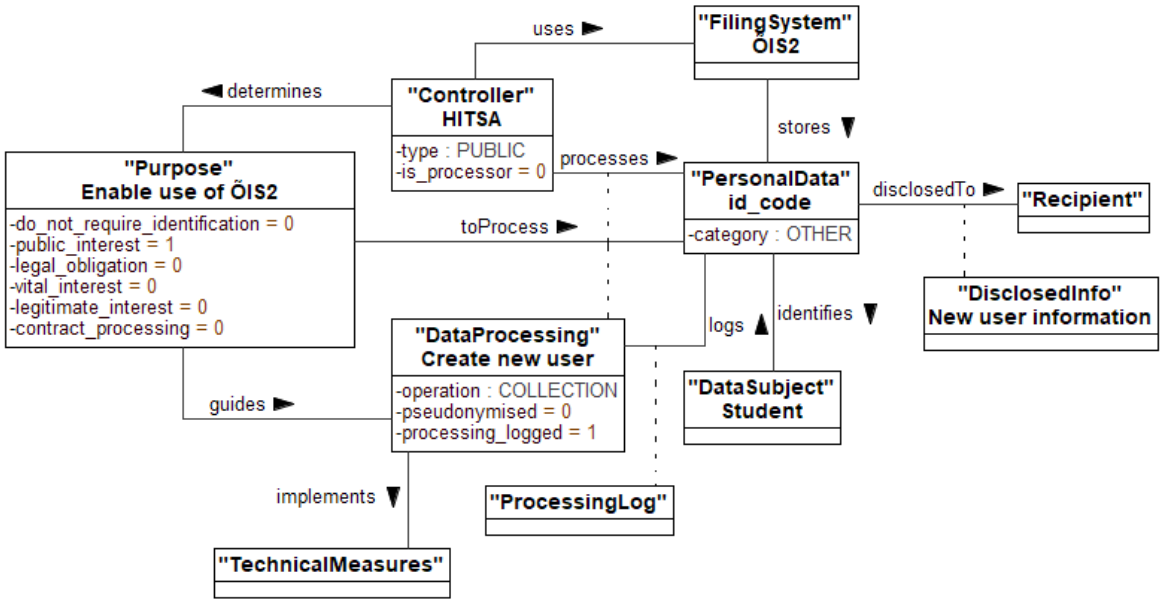


**Figure 24.** Example of Extraction Rule 8 (current)

Although with the current example, there is no information about whether the `Recipient` is an entity within the EU or outside, this is information that should be extracted from the controller. The current Model, however, does address this matter. It does not influence the extraction result if a `Recipient` would reside in a third country.

### 5.2.8.2 Refined Model

The refined Model represents the `Recipient` and disclosure of personal data in a similar manner to the current Model (`PersonalData<<disclosedTo>>Recipient`). The refined Model, however, addresses the fact whether data is transferred inside EU Member States or to a third country. Class `DataProcessing` has an attribute `-third_country`. In this hypothetical scenario, we assume that ÕIS2 sends new user information to a `Recipient` residing in Ukraine because the user is a Ukrainian national. In this scenario, the attribute `-third_country` value is 1. This in turn triggers the question whether the data transfer has a legal ground. In the refined Model, this is represented as class `LegalGroundDataTransfer` (see 4.2.3). In this hypothetical scenario, the assumption is that the data transfer takes place on the basis of appropriate safeguards under [1, art. 46(2)(a)] - represented in 4.2.3 as gate-way `Transfer subject to appropriate safeguards` XOR `Yes`).

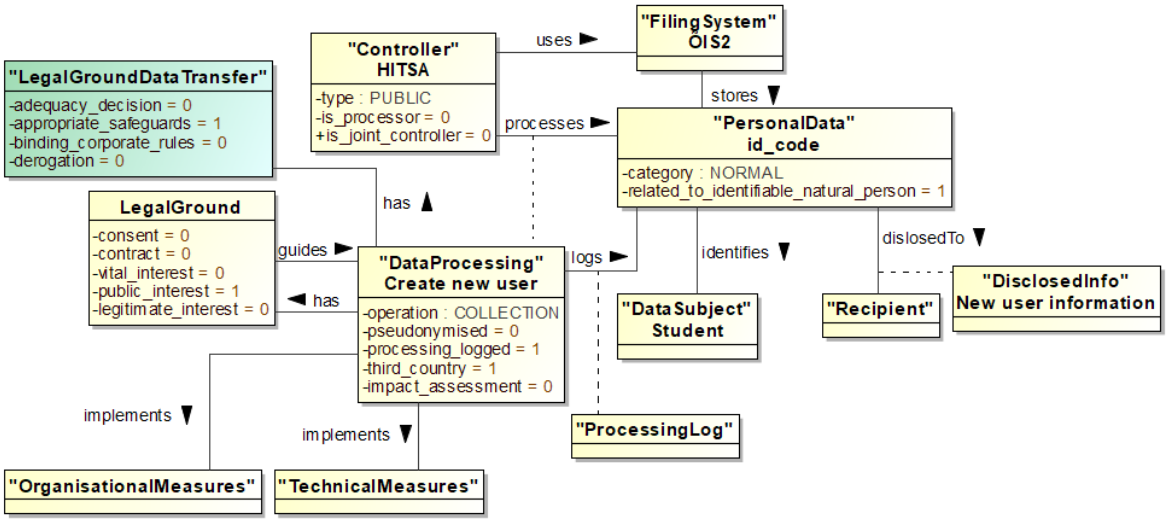


**Figure 25.** Example of Extraction Rule 8 (refined) if data is transferred to a third country

### 5.2.9 Extraction Rule 9: Principles of Processing

Information about the adherence to the principles of processing is not represented in the business process model and needs input from the controller. Moreover, adherence to the principles is rather an overall assessment considering all the aspects and input described above and requires further input from the DPO if it is appointed in accordance with [1, art. 37]. As such, this task is manual.

#### 5.2.9.1 Current Model

Adherence to the principles of processing cannot be extracted in the business process Model. It is rather an overall assessment considering all the above and requires further input from the controller. However, as the method presented in 5.1 describes the compliance process as an iterative process, the aim of the controller is to guarantee and demonstrate compliance to the data processing principles set out in [1, art. 5(1)].

However, adherence to the data processing principles cannot be modelled using the current Model as there are no corresponding classes or attributes.

#### 5.2.9.2 Refined Model

The refined Model represents data processing principles as class `PrinciplesOfProcessing` which is associated with the class `Controller` (`Controller<<isAccountable>>PrinciplesOfProcessing`). This represents the logic set out in [1, art. 5(2)] stating that controller must demonstrate compliance with the data processing principles. The adherence to the principles of processing must be presented for all processing activities (`DataProcessing` instances). In the current case, it is assumed that all principles of processing (attributes of class `PrinciplesOfProcessing`) are fulfilled. This assumption must, however, be validated with the controller and a DPO (if appointed). If any of the principles is not fulfilled (e.g. attribute `-data_minimisation = 0`), the iterative method set out in 5.1.1 mandates the controller to review the business process and its model to guarantee compliance with the GDPR.

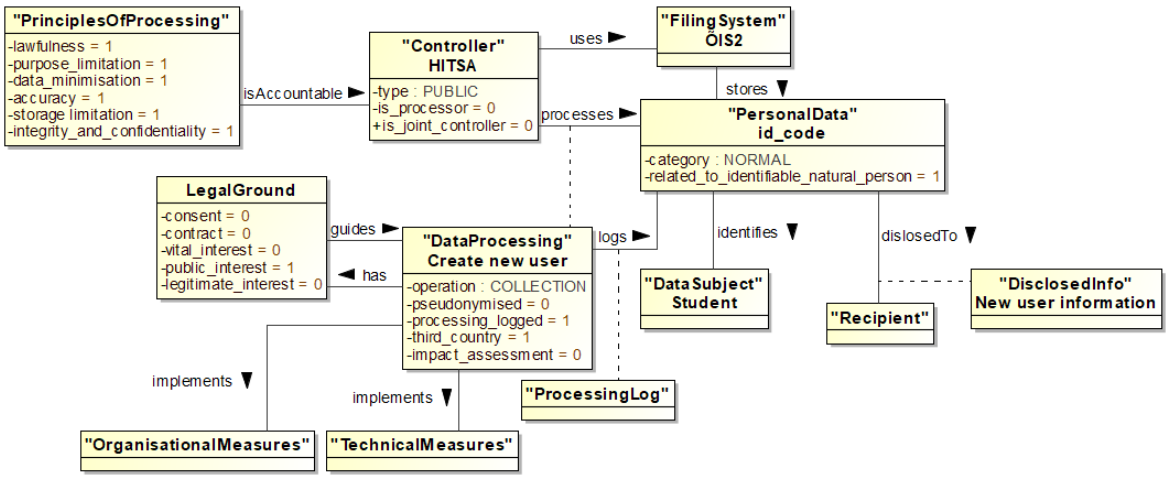


**Figure 26.** Example of Extraction Rule 9 (refined)

### 5.2.10 Extraction Rule 10: Data Subject Rights

In the context of data subject right extraction, it is assumed that a mechanism exists for evaluation of data subject right implementation in the ÕIS2 system. Data subject rights each have their own scope of application and the processing activities that need to be conducted by the controller and processor for such implementation vary [26]. Therefore, a business process model should exist for each right enforcement. In the context of this thesis, a business process model for the right of rectification is constructed (see Figure 27). It is assumed that the ÕIS2 user wishes to rectify its ID code in ÕIS2 and uses his right of rectification under Article 16 of the GDPR to do so. It is also assumed that the user presents relevant proof of identity and proof of correct date of birth together with the request for rectification.

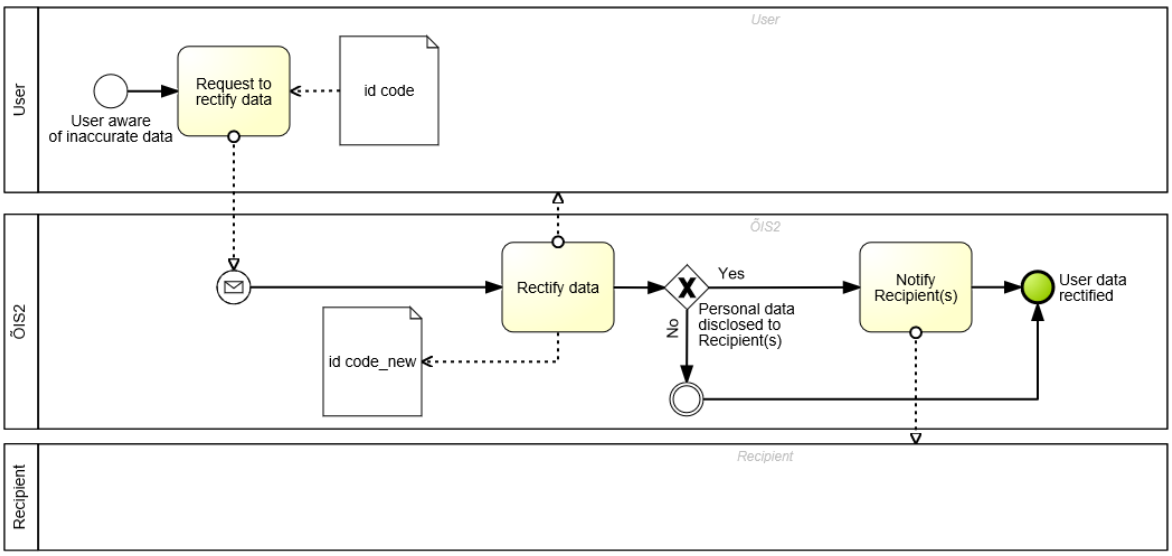


**Figure 27.** Process for right of rectification

#### 5.2.10.1 Current Model

Although Article 16 of the GDPR is covered in the current Model, it must be noted that the current Model has some gaps in data subject rights. The current Model does not cover the right of information [1, art. 13, 14], right to object [1, art. 21] and the right not to be subject to automated decision-making [1, art. 22].

In the current Model, the class `Right` is represented as generalization of all rights covered in the Model. In the example of right of rectification, the Model covers [1, art. 19] with the association `Rectification<<triggers>>Notification` and `Notification<<discloses>>Recipient`.

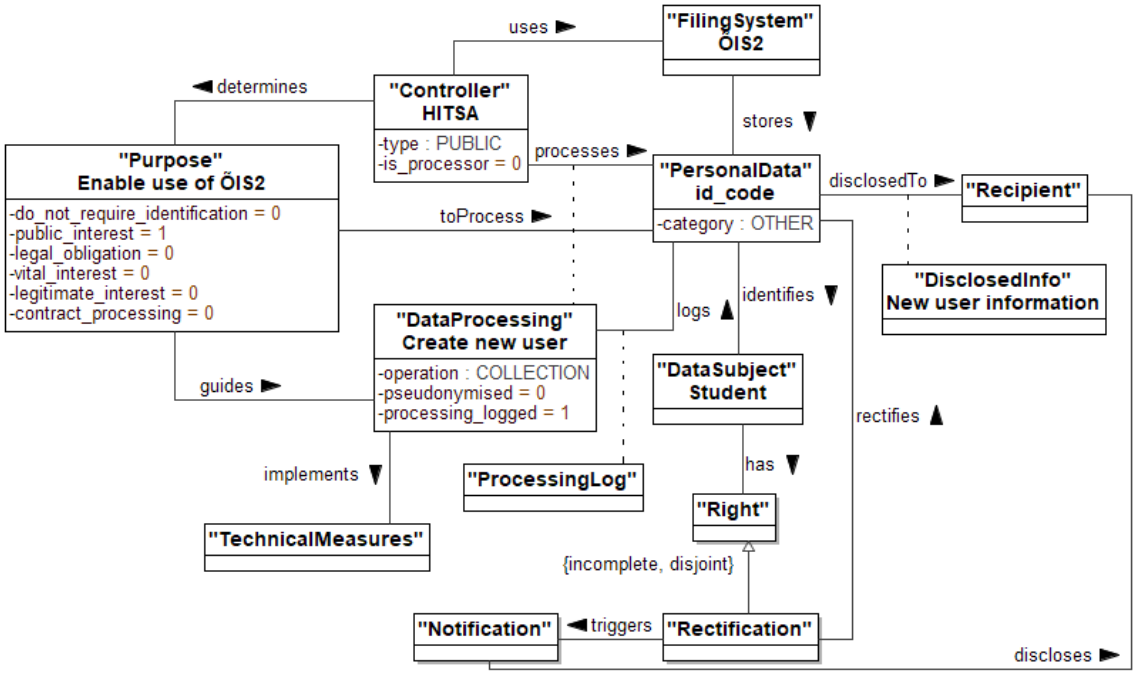


**Figure 28.** Example of Extraction Rule 10 (current)

### 5.2.10.2 Refined Model

The refined Model adds attributes to the class `Right` which cover all data subject rights in the GDPR. The refined Model covers three more rights omitted from the current Model. However, in the example at hand, it is irrelevant. In the current example, the difference lies with the attributes of the class `Right`. The attributes added in the refined Model are: -`identity_confirmed` which we assume to have value 1, -`action_taken_within_30_days` which we also assume to have value 1 and attribute `-free of charge` with value 1. The refined Model includes one extra attribute not used at this point: -`informed_datasubject_when_action_not taken: Boolean`. It was not used as action was taken by the controller in the example at hand.

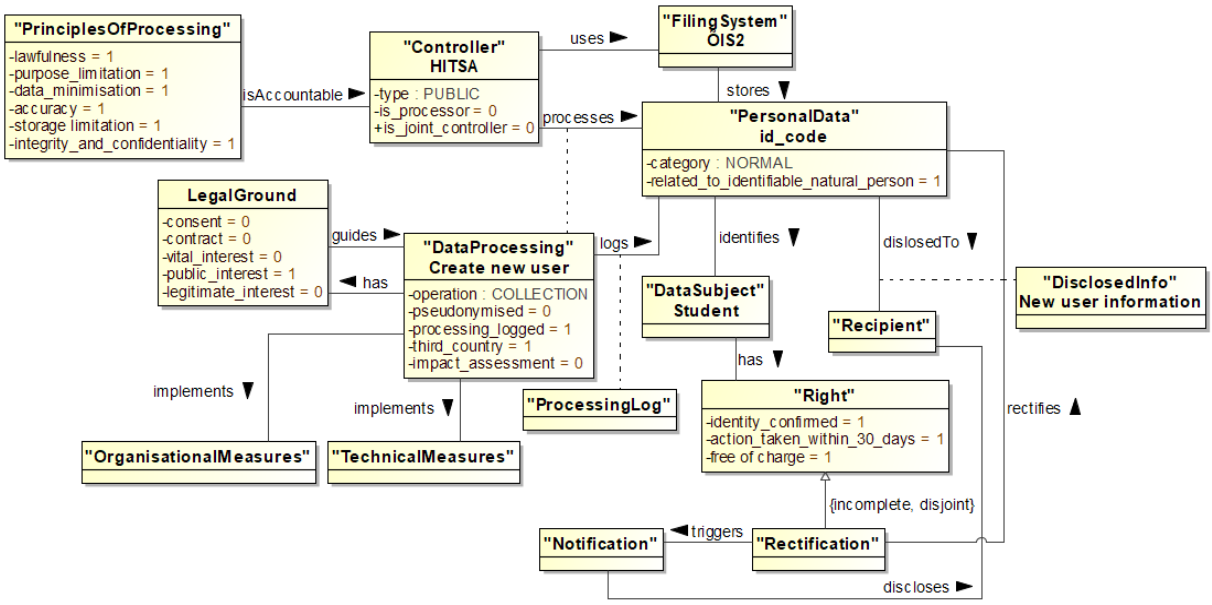


**Figure 29.** Example of Extraction Rule 10 (refined)

## 5.3 Threats to Validity

The results of the application of the running business process example can be counted as positive, however, threats to the validity of the results are still present:

1) The validation was conducted on one business process. In order to achieve better validation, more business process need to be validated to ensure the validity of the results.
2) The application of the refined Model to a business process in 5.2 was conducted solely by the author. Although a legal expert by background and experienced as a DPO, the validation of the results would benefit from having been reviewed by more legal experts.
3) The validation was conducted by a person having a background in data protection law and GDPR. Being a GDPR compliance model, the refined DPOE Model requires some background in data protection law. If applied by a person without this expertise, there might be a threat to the validity of the results.

## 5.4 Results

The purpose of refining the current Model was to help organizations to best avoid administrative fines imposed under the GDPR. For this, the current Model was refined using the method described in section 3.2.1. In section 5.2, the current and refined Models were applied to a running example business process model. In this section, the results rendered by the application of these Models to an actual business process model are compared to answer the SUBQ3.

Although the legal completeness of the Models in terms of GDPR article coverage differ (see 4.3), the actual aim of the application of the Models to the business process is to verify whether the refined Model would enable the controller to avoid fines to a bigger extent than the current Model does. This will be discussed in the sub-sections below.

### 5.4.1 Actors

The refined Model proposes changes to the classes `Controller` (attribute `+is_joint_controller: Boolean`) and `Processor` (attributes `-is_controller: Boolean` and

-has_authorisation: Boolean). This adds three GDPR requirements to the refined DPOE Model – articles 26, 28(10) and 28(3) – compared to the current Model. All of these requirements fall under Article 83(4)(a) of the GDPR and, therefore, improve the legal completeness of the Model by adding articles which' infringement may bring about administrative fines.

The refined Model also adds two new actors - Representative (Article 27 of the GDPR) and DataSubject. The latter was present in the current Model, but not seen as an Actor. This is seen as a deficiency of the current Model by the author and is part of the legal validation undertaken by the author. The addition of these two actors does not, however, influence the results of the running example.

### 5.4.2 Personal Data, Data Subject, Filing System and Records of Processing

Extraction Rules 2, 3 and 5 provided, in principle, similar results.

In terms of personal data and data subject (Extraction Rule 2; see also 5.2.2), the refined Model adds one attribute to class PersonalData (-related_to_identifiable_natural_person: Boolean) which is key for deciding whether a data object constitutes as "personal data" under the GDPR or not. As discussed above, this attribute is probably assumed in the current Model, but not explicitly stated. Therefore, this addition provides legal validation of the current Model and is not a significant change.

In case of FilingSystem (Extraction Rule 3) and ProcessingLog (Extraction Rule 5), the instantiation of the running example did not provide any changes (except to the attributes of other classes related to it (PersonalData, Controller and DataProcessing).

### 5.4.3 Processing Activities

Regarding data processing activities (Extraction Rule 4), the refined Model proposes significant additions.

The refined Model includes one important element lacking in the current Model – the obligation to verify whether a DPIA or prior consultation needs to be conducted or not. As failing to conduct a DPIA or prior consultation may bring about administrative fines under Article 83(4)(a) of the GDPR, it is certainly a significant inclusion compared to the current Model. In order to verify whether the obligation to conduct a DPIA or prior consultation must be undertaken, the controller needs to turn to the business process model set out in 4.2.1. In the current case, the obligation to perform a DPIA was not confirmed (represented as attribute -impact_assessment of class DataProcessing value = 0; see 5.2.4).

However, if it were to be the opposite (i.e. when attribute -impact_assessment of class DataProcessing value = 0), the refined Model includes a class <<Artifact>>DataProtectionImpactAssessment with attributes covering Article 35(7)(a)-(d) of the GDPR. Therefore, the refined Model incorporates the obligation to conduct a DPIA or prior consultation which may be considered as significant additions.

Also, the refined Model adds three new attributes: -impact_assessment: Boolean, -data_breach: Boolean and -third_country: Boolean. Although, as the business process example did not include information about this, the attributes did not provide any significance. However, under Extraction Rule 8 (see 5.2.8), a hypothetical case was presented where Recipient would be a third country (attribute -third_country of class DataProcessing value = 1). In that hypothetical scenario, this triggered the applicability criteria set out in 4.2.3 to verify whether the data transfer to the third country has a legal basis or not.

Although it was concluded that the new attributes were not of significance for the example business process, they do cover a gap in the current Model by adding Articles 33, 34, 35,36 and Chapter V of the GDPR that were not covered by the current Model. As such, the additions will increase the legal completeness of the Model and helps the controller to avoid administrative fines under the GDPR.

### 5.4.4 Legal Ground

The refined Model validates the way how legal ground for processing (Extraction Rule 6) is presented in the Model. Also, it includes the legal grounds for processing special categories of data that are not covered in the current Model.

The current Model views the legality of data processing only from the angle of the consent. Consent is indeed one legal ground under the GDPR [1, art. 6], but it is neither the most important nor the main legal ground. As such, the logic how legal grounds for processing are presented in the current Model is incorrect from the legal perspective. The refined Model includes a class `LegalGround` connected to data processing with the association `<<has>>` (`DataProcessing<<has>> LegalGround`). `LegalGround` also guides `DataProcessing` as it sets the limits and describes the purpose of `DataProcessing`. Therefore, the association `LegalGround<<guides>>DataProcessing` is added to the refined Model.

Therefore, the refined Model validates the current Model from the legal perspective. This is exemplified by the application of the current Model to the business process – the extraction results in the reading of the Model where HITSA determines the `Purpose` which is a legal ground (attribute `public_interest`). In comparison, the application of the same business process to the refined Model renders the result where `DataProcessing` has a `LegalGround` (`-public_interest = 1`) which guides `DataProcessing`. This better represents the principle of lawfulness set out in [1, art. 5(1)(a)].

### 5.4.5 Measures

The refined Model provides significant changes to the current Model in regard to measures (Extraction Rule 7).

The refined Model includes class `OrganisationalMeasures` described in Article 32(1) of the GDPR next to technical measures. Therefore, the refined Model adds one element the controller needs to follow in order to comply with the GDPR. As such, it is considered as a significant addition from the perspective of administrative fines as Article 83(4)(a) of the GDPR includes Article 32 as one of the articles which' infringement may bring about fines.

### 5.4.6 Disclosure

The refined Model incorporates data transfers to third countries. As such, the refined Model includes Chapter V of the GDPR and this is a significant contribution in light of Article 83(5)(c) of the GDPR.

The refined Model includes attribute `-third_country` of the class `DataProcessing` which represents the fact that the `Recipient` to whom the personal data is disclosed is in a third country. This triggers the applicability criteria set out in 4.2.3 to verify the legal basis.

Therefore, the inclusion of attribute `-third_country` with the class `LegalGroundDataTransfer` adds to the refined Model Articles 45(1), 46(1), 46(3), 47(1) and 49(1) of the GDPR not covered in the current Model. Infringement of any of these articles may bring about a fine of up to 20,000,000 EUR under Article 83(5)(c) of the GDPR. Therefore, the additions are important and enhance the legal completeness of the Model.

### 5.4.7 Principles of Processing

The refined Model includes principles of processing personal data (Article 5(1) of the GDPR) omitted altogether from the current Model (Extraction Rule 9). Incompliance with Article 5(1) of the GDPR may bring about maximum fines under Article 83(5)(a) of the GDPR. The inclusion of class `PrinciplesOfProcessing` associated with class `Controller` with the association `isAccountable` covers both Articles 5(1) and 5(2) of the GDPR. Therefore, the refined Model significantly improves the controller's aspirations to avoid fines under the GDPR.

### 5.4.8 Data Subject's Rights

Application of the right of rectification process (5.2.10) to the current and refined Models enhances the legal completeness of the Model by adding attributes covering Articles 12(3)-12(6) of the GDPR (`-identity_confirmed: Boolean, -action_taken_within_30_days: Boolean, -free_of_charge: Boolean, -informed_datasubject_when_action_not_taken: Boolean`). Not following these legal requirements may bring about maximum fines under Article 83(5)(b) of the GDPR. Therefore, the inclusion of the attributes to class `Right` increased the legal completeness of the refined Model.

Outside the ÕIS2 login example, the refined Model significantly improves the Model by including three rights not covered in the current Model – right of information (Articles 13 and 14 of the GDPR; class `Information`), right to object (Article 21 of the GDPR; class `Object`) and the right not to be subject to automated decision-making (Article 22 of the GDPR; class `NotToBeSubjectToAutomatedDecision`). Although not relevant in the context of the running example, the inclusion of these rights adds significant value in terms of avoiding administrative fines as incompliance could lead to maximum administrative fines under Article 83(5)(b) of the GDPR.

## 5.5 Summary

The application of the refined Model to the running example (ÕIS2 login) improves the legal completeness of the DPOE Model as it covers 13 GDPR articles not covered with the current Model. Namely, Articles 4(1), 5(1), 5(2), 12(3), 12(4), 12(5), 12(6), 26, 28(3), 28(10), 32(1), 35(1) and 35(3) of the GDPR. As these articles fall under Articles 83(4) and 83(5) of the GDPR, they may be considered important additions considering criteria for refinement. As such, the refined Model improves the legal completeness (i.e. GDPR article coverage) by including more GDPR articles relevant for avoiding fines.

If hypothetical scenarios would be considered (i.e. a DPIA needs to be made and data is transferred to a third country), the value of the refined Model would be even more apparent as the refined Model would then cover 19 more GDPR articles which all would be important requirements under Articles 83(4) or 84(5) of the GDPR. These are Articles 4(1), 5(1), 5(2), 12(3), 12(4), 12(5), 12(6), 26, 28(10) and 28(3), 32(1), 35(1), 35(7), 45(1), 46(1), 46(2), 46(3), 47(1) and 49(1) of the GDPR.

# 6 Conclusion

The thesis aimed to improve the legal completeness (i.e. GDPR article coverage) of the DPOE Model and validate the Model based on Articles 83(4) and 83(5) of the GDPR to help organizations avoid administrative fines that could lead up to 20,000,000 EUR.

## 6.1 Limitations and Lessons Learned

One of the limitations of the refined DPOE Model is that it represents the GDPR and does not consider the national implementation of it. As GDPR leaves room for Member States to agree on some aspects of it plus some of the legal grounds for processing arise from national laws, the refined DPOE Model helps the controller and the DPO to an extent – if national laws add on top of the GDPR, there could be other relevant aspects the controller needs to take into account to achieve compliance with the data protection rules.

Although the aim of the DPOE would be to semi-automate the GDPR compliance process, adding more GDPR articles to the Model as was done with the refined DPOE Model increased the legal completeness of the Model on the one hand, but also increased the amount of manual input required from the controller and the DPO from the other hand. Therefore, the manual input needs also need to be accommodated to the future DPOE solution.

One of the limitations was also be the business process used as an example to test the Models. The advantages of the refined Model could be better exemplified if a more complex BPMN model was used – it could bring out important disadvantages and weaknesses which could help refine the DPOE Model even further.

## 6.2 Answers to Research Questions

**SUBQ1**: **What are the criteria for refining the DPOE Model?**

The criteria for refining the DPOE Model arise from Articles 83(4) and 83(5) of the GDPR. These articles define essentially the key articles which' compliance helps organizations to avoid fines under the GDPR. These are Articles 5, 6, 7, 8, 9, 11, 12-22, 25-39, 42, 43, 44-49. Infringement of these articles may bring about fines up to 20,000,00 EUR. In total, with all the paragraphs of articles mentioned above, 191 articles (e.g. Article 5 paragraph 1 is considered as one article)) are in scope of this thesis.

**SUBQ2**: **What is the legal completeness (i.e. GDPR article coverage) of the current DPOE Model compared to the refined Model considering the criteria of refinement?**

Although there are 191 GDPR articles in scope, not all these articles contain specific legal requirements for organizations. Many of these articles mandate the European Commission or the Member States, not the controller. Some are articles that contain generic best effort clauses that are not fit for modelling. Therefore, the inclusion and exclusion criteria were established to include GDPR articles that: a) contain a specific legal requirement obliging controllers and processors; and b) enable the modelling of article mentioned in a) (see 3.2.1.1 and 3.2.1.2). Also, some of the articles that described the applicability of certain requirements (e.g. if a data breach occurs, then a notification must be made to the supervisory authority or the data subjects) and met the Exclusion Criteria, were still modelled under section 4.2 as the omission of these would have significantly decreased the value of the refined Model. As a result of the refinement process, the refined Model covers 75 key articles that meet the inclusion criteria. At the same time, the current DPOE Model covers 26 GDPR articles. Thus, the refined Model covers 49 more GDPR articles (25% more than the current Model). The GDPR article coverage of both Models is set out in Table 10 (see 4.3).

**SUBQ3**: **What is the feasibility of the refined DPOE Model?**

The application of the refined Model to the running example (ÕIS2 login) improves the legal completeness (i.e. GDPR article coverage) of the DPOE Model as it covers 13 GDPR articles not covered with the current Model (4(1), 5(1), 5(2), 12(3), 12(4), 12(5), 12(6), 26, 28(3), 28(10), 32(1), 35(1), 35(3)). As these articles fall under Articles 83(4) and 83(5) of the GDPR, they are important additions and increase the GDPR article coverage of the refined Model. As such, the legal completeness (i.e. GDPR article coverage) of the DPOE Model is enhanced.

If hypothetical scenarios would be considered (i.e. a DPIA needs to be made and personal data is transferred to a third country), the value of the refined Model would be more apparent as the refined Model would then cover 19 (4(1), 5(1), 5(2), 12(3), 12(4), 12(5), 12(6), 26, 28(10) and 28(3), 32(1), 35(1), 35(7), 45(1), 46(1), 46(2), 46(3), 47(1) and 49(1)) more articles which all would be important requirements under Articles 83(4) or 84(5) of the GDPR. Thus, the refined Model would help organizations to avoid fines under the GDPR to a greater extent than under the current Model.

**MRQ**: **How should the DPOE Model be refined considering the administrative fines?**

The key focus of many organizations is to achieve compliance under the GDPR. One way of approaching this aim is to look at the articles which incompliance may bring about fines. This thesis looked at this way of refining the DPOE Model to introduce changes to the current Model which was taken as a basis for the refinement.

The refined DPOE Model introduced the following key changes:

1) the structure and logic of the legal ground for processing (inclusion of classes `LegalGround`, `LegalGroundSpecialCategory` and `LegalGroundDataTransfer`) has changed. `DataProcessing<<has>>LegalGround` which in turn `<<guides>>DataProcessing`. This is in line with the legal discourse.
   Also, the addition of `LegalGroundSpecialCategory` and `LegalGroundDataTransfer` include the legality of processing special categories of data [1, art.9(2)] and the legality of data transfers to third countries [1, chapter V].
2) new actors introduced to the Model. The refined Model includes `DataSubject` – a key entity without whom personal data processing does not exist – as an actor. Also, the actor `Representative` is included as an actor.
3) all the data subject rights are now included. The current Model did not include the right of information, the right to object and the right not to be subject to automated decision-making. The omission of three data subject rights is a serious deficit of the current Model and does not enable organization to avoid fines under the GDPR. Also, the class `Right` includes four attributes that cover articles 12(3)-12(6) of the GDPR and help organizations in avoiding fines.
4) Data processing principles and the principle of accountability [1, art. 5] are included in the Model. As the non-compliance of the data processing principles is a major infringement under [1, art. 83(5)(a)], the inclusion is of significant value.
5) the obligation to conduct a DPIA and prior consultation is included. Class `<<Artifact>>DataProtectionImpactAssessment` with the applicability criteria set out in 4.2.1 enable the organisation to decide whether a DPIA or prior consultation needs to be conducted and if so, what are the content requirements.

6) besides technical measures, the DPOE Model now mentions organizational measures (class `OrganisationalMeasures`) that are mandated under [1, art. 32(1)] and key elements under [1, art. 25(1) and 25(2)]. The omission of one class of measures is a significant deficit as the non-compliance may bring about fines.
7) `DataProcessing` includes three new attributes (`-impact_assessment: Boolean,-data_breach: Boolean` and `-third_country: Boolean`) incorporating Articles 35, 33 and 34 and 45(1), 46(1), 46(3), 47(1) and 49(1) of the GDPR.
8) data breach and data breach notification (class `DataBreachNotification`) are added to the refined Model. This inclusion covers [1, art. 33,34]. Failure to notify the supervisory authority or, in certain scenarios (see 4.2.4), brings about a fine under [1, art. 83(4)(a)]. Therefore, the inclusion is of significant value considered the purpose of refinement.

As a result, it is concluded that introducing these changes would help organizations to avoid fines under the GDPR to a greater extent than under the current Model as the GDPR article coverage has increased from 26 to 75 GDPR articles with the focus of avoiding fines (i.e. with the criteria of refinement). Therefore, the modification of the DPOE Model from the administrative fines' perspective helps organizations to avoid fines.

### 6.3 Conclusion

As a result of the thesis, the DPOE Model's maturity is enhanced and the legal completeness (i.e. GDPR article coverage) of the Model is greater as it covers more GDPR articles. The results in 5.4 indicate that the application of the refined Model to an actual business process model incorporates more legal requirements relevant for compliance compared to the current DPOE Model. As such, the refined DPOE Model helps organizations to avoid fines under the GDPR to a greater extent.

### 6.4 Future Work

Future work that could be considered based on the limitations (6.1) are:

1) creating national or sector specific GDPR models extending the refined DPOE Model by adding requirements from Member State laws;
2) finding ways to semi-automate user input required from the controller;
3) application of the refined DPOE Model to more business processes to further filter out advantages, disadvantages and weaknesses of the refined Model.

# 7 References


1. Regulation (EU) 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). OJ L 119, 4.5.2016, p. 1–88.
2. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. OJ L 281, 23.11.1995, p. 31–50.
3. Kuner C., Bygrave L. and Docksey C. Draft commentaries on 10 GDPR articles (from Commentary on the EU General Data Protection Regulation, OUP 2019). Commentary on the EU General Data Protection Regulation (GDPR) (2019). Available: https://works.bepress.com/christopher-kuner/1/ [Accessed 23.04.2019].
4. Tom J., Sing E. and Matulevičius R. (2018) Conceptual Representation of the GDPR: Model and Application Directions. In: Zdravkovic J., Grabis J., Nurcan S., Stirna J. (eds) Perspectives in Business Informatics Research. BIR 2018. Lecture Notes in Business Information Processing, vol 330. Springer, Cham.
5. Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, signed at Lisbon, 13 December 2007. OJ C 306, 17.12.2007, p. 1–271.
6. Treaty establishing the European Community. Official Journal C 325, 24/12/2002 P. 0033 – 0184.
7. Handbook on European Data Protection Law: 2018 edition. European Union Agency for Fundamental Rights. Available: https://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law [Accessed 24.04.2019].
8. Mayer-Schönberg, V and Padova, Y. Regime Change? Enabling Big Data Through Europe's New Data Protection Regulation. The Columbia Science & Technology Law Review, Vol XVII (2016), p 321. Available: http://stlr.org/download/volumes/volume17/SchonbergerPadova.pdf [Accessed 23.04.2019].
9. Zarsky T. Incompatible: The GDPR in the Age of Big Data (2017). Seton Hall Law Review, Vol. 47, No. 4(2), 2017. Available: https://ssrn.com/abstract=3022646 [Accessed 23.04.2019].
10. Moerel, E.M.L. and Prins, J.E.J. (Corien). Privacy for the Homo Digitalis: Proposal for a New Regulatory Framework for Data Protection in the Light of Big Data and the Internet of Things (May 25, 2016). Available: https://ssrn.com/abstract=2784123 or http://dx.doi.org/10.2139/ssrn.2784123 [Accessed 23.04.2019].
11. Purtova N. The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law (2017). 2018 Law, Innovation and Technology 10(1). Available https://ssrn.com/abstract=3036355 [Accessed 23.04.2019].
12. Article 29 Working Party opinion 4/2007 on the concept of personal data, 20 June 2007 ('WP 136'). Available: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf [Accessed 23.04.2019].
13. Article 29 Working Party opinion 1/2010 on the concepts of "controller" and "processor", 16 February 2010 ('WP 169'). Available: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf [Accessed 23.04.2019].

14. Article 29 Working Party opinion 3/2010 on the principle of accountability ('WP173'). Available: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp173_en.pdf [Accessed 23.04.2019].
15. Article 29 Working Party Guidelines on consent under Regulation 2016/679 ('WP259'). Available: https://iapp.org/media/pdf/resource_center/20180416_Article29WPGuidelinesonConsent_publishpdf.pdf [Accessed 23.04.2019].
16. Contract, ICO website. Available: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/contract/ [Accessed 23.04.2019].
17. Judgement of the European Court of Justice, C-524/06, *Heinz Huber v. Bundesrepublik Deutschland* [GC], 16 December 2008.
18. Article 29 Working Party (2014), Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, 4 April 2014. Available: https://fia.org/sites/default/files/uploaded/Excerpts%20-%20Opinion%2006-2014%20on%20the%20notion%20of%20legitimate%20interests%20of%20the%20....pdf [Accessed 23.04.2019].
19. Judgment of the European Court of Justice (C-131/12), *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, 13 May 2014.
20. European Commission website regarding adequacy decisions. Available: https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en [Accessed 23.04.2019].
21. French Data Protection Authority (CNIL) Data Protection Impact Assessment Tool. Available: https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assesment[Accessed 23.04.2019].
22. Robol M., Salnitri M., Giorgini P. (2017) Toward GDPR-Compliant Socio-Technical Systems: Modeling Language and Reasoning Framework. In: Poels G., Gailly F., Serral Asensio E., Snoeck M. (eds) The Practice of Enterprise Modeling. PoEM 2017. Lecture Notes in Business Information Processing, vol 305. Springer, Cham.
23. Diamantopoulou, V., Angelopoulos, K., Pavlidis, M., Mouratidis, H.: A metamodel for GDPR-based privacy level agreements. Available: http://ceur-ws.org/Vol-1979/paper-08.pdf [Accessed 23.04.2019].
24. Becker, J., Knackstedt, R., Braeuer, S., Heddier, M.: Integrating Regulatory Requirements into Information Systems Design and Implementation. Available: https://pdfs.semanticscholar.org/977f/d7ca0da48fa9ed72e990b3bc19a3d4dfd316.pdf [Accessed 23.04.2019].
25. Celebi, I.: Privacy Enhanced Secure Tropos: A Privacy Modelling Language for GDPR Compliance. Available: https://comserv.cs.ut.ee/home/files/Celebi-Cybersecurity-2018.pdf?study=ATILoputoo&reference=1749FCFE6ACD75EF3381E5B2294EA55C3D1E546F [Accessed 23.04.2019].
26. Sing, E.: A Meta-Model Driven Method for Establishing Business Process Compliance to GDPR (Tartu, 2018). Available: https://comserv.cs.ut.ee/home/files/sing_softwareengineering_2018_10.pdf?study=ATILoputoo&reference=9DF06178055B832A7E71C23151B07F3A9C4DDC72 [Accessed 23.04.2019].

27. Pullonen P., Matulevičius R., Bogdanov D. (2017) PE-BPMN: Privacy-Enhanced Business Process Model and Notation. In: Carmona J., Engels G., Kumar A. (eds) Business Process Management. BPM 2017. Lecture Notes in Computer Science, vol 10445. Springer, Cham.
28. Universitas Tartuensis. September 2018/8. Available: https://www.ajakiri.ut.ee/taxonomy/term/745 [Accessed 23.04.2019].
29. Study Regulation of the University of Tartu. Available: https://www.ut.ee/studreg [Accessed 18.03.2019].
30. Data Protection Policy of the University of Tartu. Available: https://www.ut.ee/en/data-protection-policy [Accessed 18.03.2019].

# Appendix

## I. Articles Meeting the Exclusion Criteria

| Rule | GDPR article |
|---|---|
| **Exclusion Rule 1** | 6(4), 8(2), 11(1), 11(2), 12(7), 12(8), 15(2), 15(3), 18(2), 18(3), 20(3), 22(3), 26(2), 44 |
| **Exclusion Rule 2** | 4(23), 6(2), 6(3), 8(3), 9(4), 25(3), 27(5), 28(7), 28(8), 35(4), 35(5), 35(6), 36(4), 36(5), 37(4), 38(5), 39(1), 39(2), 42(1), 42(2), 42(3), 42(4), 42(5), 42(6), 42(7), 42(8), 43(1), 43(2), 43(3), 43(4), 43(5), 43(6), 43(7), 43(8), 45(2), 45(3), 45(4), 45(5), 45(6), 45(7), 45(8), 46(4), 47(3), 49(5) |
| **Exclusion Rule 3** | 4(12), 4(20), 7(1), 9(2)*, 14(5), 17(3), 21(3), 21(6), 22(2), 22(4), 26(3), 27(2), 28(4), 29, 30(5), 33(1)*, 34(1)*, 34(3), 34(4)*, 35(1)*, 35(3)*, 35(10), 36(1)*, 44*, 45(1)*, 46(1)*, 46(2), 46(3), 47(1)*, 49(1)* |
| **Exclusion Rule 4** | 9(3), 13(2), 13(3), 13(4), 14(2), 14(3), 14(4), 15(4), 20(2), 20(4), 21(4), 21(5), 27(3), 27(4), 28(1), 28(2), 28(5), 28(6), 28(9), 30(3), 32(2), 32(3), 32(4), 33(2), 33(3)*, 33(4), 33(5)*, 34(2)*, 35(2), 35(8), 35(9), 35(11), 36(2)*, 36(3), 37(2), 37(3), 37(5), 37(6), 38(1), 38(2), 38(3), 38(4), 38(6), 45(9), 46(5), 47(2), 48, 49(2), 49(3), 49(4), 49(6) |

* - article modelled in section 4.2 (applicability criteria).

## II. Glossary

| | |
|---|---|
| 1995 Directive | Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data |
| BPMN | Business Process Model and Notation |
| CJEU | European Court of Justice |
| CNIL | The French Data Protection Authority (*Commission nationale de l'informatique et des libertés*) |
| DPIA | Data Protection Impact Assessment |
| DPO | Data Protection Officer |
| DPOE | Data Protection Observation Engine, a software tool envisioned by the researchers of University of Tartu for semi-automated GDPR compliance |
| EUR | Euro (currency) |
| GDPR | Regulation (EU) 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) |
| PESTOS | Privacy Enhanced Secure Tropos |
| PLA | Privacy level agreement |
| STS | Socio-technical security |
| UML | Unified Modelling Language |

## III. Licence

**Lihtlitsents lõputöö reprodutseerimiseks ja lõputöö üldsusele kättesaadavaks tegemiseks**

Mina, **Kaspar Kala**,
(*autori nimi*)

1. annan Tartu Ülikoolile tasuta loa (lihtlitsentsi) enda loodud teose
**Refinement of the General Data Protection Regulation (GDPR) Model: Administrative Fines Perspective**,
(*lõputöö pealkiri*)

mille juhendaja on Raimundas Matulevičius,

reprodutseerimiseks eesmärgiga seda säilitada, sealhulgas lisada digitaalarhiivi DSpace kuni autoriõiguse kehtivuse lõppemiseni.

1. Annan Tartu Ülikoolile loa teha punktis 1 nimetatud teos üldsusele kättesaadavaks Tartu Ülikooli veebikeskkonna, sealhulgas digitaalarhiivi DSpace kaudu Creative Commonsi litsentsiga CC BY NC ND 3.0, mis lubab autorile viidates teost reprodutseerida, levitada ja üldsusele suunata ning keelab luua tuletatud teost ja kasutada teost ärieesmärgil, kuni autoriõiguse kehtivuse lõppemiseni.

2. Olen teadlik, et punktides 1 ja 2 nimetatud õigused jäävad alles ka autorile.

3. Kinnitan, et lihtlitsentsi andmisega ei riku ma teiste isikute intellektuaalomandi ega isikuandmete kaitse õigusaktidest tulenevaid õigusi.

Tartus, **15.05.2019**