A Method for Managing GDPR Compliance in Business Processes

Chapter *in* Lecture Notes in Business Information Processing · August 2020

DOI: 10.1007/978-3-030-58135-0_9

CITATIONS
16

READS
1,642

4 authors, including:

Raimundas Matulevičius
University of Tartu
189 PUBLICATIONS **2,679** CITATIONS
SEE PROFILE

Jake Tom
University of Tartu
6 PUBLICATIONS **128** CITATIONS
SEE PROFILE

Eduard Sing
University of Tartu
2 PUBLICATIONS **47** CITATIONS
SEE PROFILE

A Method for Managing GDPR Compliance in Business Processes

Raimundas Matulevičius[1], Jake Tom[1], Kaspar Kala[2,3], and Eduard Sing[4]

[1] Institute of Computer Science, University of Tartu, Estonia
[2] School of Law, University of Tartu, Estonia
[3] Proud Engineers OÜ, Estonia
{rma, jaketom, kaspar.kala}@ut.ee
[4] Fujitsu Estonia AS, Estonia
ecbyu7@gmail.com

Abstract. Organisational compliance with the General Data Protection Regulation (GDPR) is a challenging task. In this paper, we present a GDPR model and its supporting method to manage compliance to the regulation in business processes. Based on a running example, we illustrate how the method is applied to extract an *as-is* compliance model that describes non-compliance issues and offers solutions to achieve process compliance. The GDPR model and its method are supported by a software tool. Their feasibility and validity are studied in a few business-oriented cases. The paper also discusses the model completeness with respect to the regulation.

Keywords: GDPR · Privacy Management · Regulation compliance · Business process modelling

1 Introduction

With the Generic Data Protection Regulation (GDPR) [1], organisations require techniques to assess and to make compliant their state of personal data processing. Regardless of industry or size, one needs to find ways to achieve and maintain the specified privacy standards. But as there is no standard approach for achieving GDPR compliance, it is important to develop an understanding of how the privacy status can be assessed. Failing to meet compliance requirements may result in administrative fines (see [6] where more than 300 cases of the administrative fines are already reported after the GDPR introduction).

In this paper, we discuss the GDPR model [7][12] and its application to achieve the compliance in business processes. The objective is to explain *how regulation compliance could be achieved using tool-supported model-based approach.* Based on the illustrative example, we present a *method to achieve the regulation compliance.* The method supports extraction of the *as-is* compliance status, explaination and reasoning of the non-compliance issues, and change of the business process model in order to resolve the non-compliance issues. In addition we discuss completeness and validity of both the GDPR model and method.

The paper is structured as follows: first we present the related work (Sect. 2). In Sect. 3 we discuss the GDPR model. In Sect. 4, the method to achieve compliance is presented using the *Tollgate* scenario. Finally, Sect. 5 discusses the contribution and future research directions.

2 Related Work

Introduction of the GDPR regulation resulted in development of methods to support the regulation compliance. In [9] authors introduce the GDPR-based privacy vocabulary for data interoperability when creating privacy policies. In [8] a data labelling model for access control of privacy-critical data is defined. It uses the Fusion/UML process to design GDPR compliant system. Elsewhere, a reference model [4] for depicting the GDPR principles is defined. It helps consolidating the regulatory and business points of view using the enterprise architecture models.

In [13] a UML representation of GDPR for assessing compliance is proposed. Authors separate between the generic and contextual variations (related to the national levels) and introduce a model driven approach to support compliance activities. The study gives a strong background for the automatic analysis, however this still remains the future work. In addition the completeness of the GDPR representation is rather limited with respect to the regulation.

3 GDPR Model

The GDPR regulation introduces the major principles for the personal data processing. But it is rather broad and leaves a room for interpretation. In Fig. 1 we present the GDPR model [7][12]. *Personal data* [1] (Art. 4(1)) is represented with the class PersonalData. Data processing [1] (Art. 4(2)) is captured with the DataProcessing class, which also covers the cross-border processing [1] (Art. 4(23)) of personal data (using member_states and main_establishment attributes).

Controllers can also be *Processors*, (see, is_processor in Controller class following the Art. 28(10)), but they can't be processor and controller at the same time. The LegalGround presents that *data processing* must have a legal ground (whether consent or other). Consent is seen as a separate class that manifests one legal ground. The LegalGround, in turn, guides DataProcessing by setting the limits to the processing of personal data. Classes LegalGroundDataTransfer, LegalGroundSpecialCategory, and DataProtectionImpactAssessment represent regulation Art. 45-59, 9(2) and 35-36 respectively. The model also includes an obligation to issue the notification in case of a data breach (see, DataBreachNotification). The ProcessingLog artefact is created to meet [1] Art. 30, which requires maintenance of records of the processing activities.

Technical measures [1] (Art. 32(1)) are represented with the TechnicalMeasures class. TechnicalMeasures has two attributes category and stereotype which, based on a taxonomy [10], could capture privacy enhancing technology means to reach privacy goals. The OrganisationalMeasures class describes how Controller

should apply the organisational measures to *Data processing*. The model also describes the data processing principles and the principle of accountability (e.g., Controller *isAccountable* to PrinciplesOfProcessing) as described in [1] Art. 5.

Rights: The GDPR model also presents the *data subjects'* rights and associations (see [7][12]). The Controller is the key actor as it is responsible for enabling the data subjects' rights (i.e., Controller *enablesExercise* on Right). The regulation [1] Art. 16 defines the right of the data subject to have his/her personal data rectified when relevant. This further links to the notification obligation [1] Art. 19. Other rights, e.g., regarding *informing*, *objecting* and *not being subject to automated decision* – cover [1] Art. 13, 14, 21 and 22 respectively.

4 Method for Achieving Compliance

The method for achieving GDPR compliance consists of four steps, presented in Fig. 2. First, one needs to check the current level of process compliance. This includes analysis of the business process and extraction of the GDPR model instance of the current state (see, *Extract AS-IS compliance model*). Next (see, *Compare two models*), one compares the extracted model to the GDPR model. The result of the third step (see, *Define compliance issues*) is a list of the non-compliance issues. Depending on these issues, one makes a decision whether the model is compliant or not. In case of non-compliance, in the fourth step one *changes the business process model* so that the non-compliance in removed from the model. The compliance checking, then, continues with the first step taking the updated business process model as the input. Below we discuss how the method for achieving regulation compliance is applied in the *Tollgate scenario*.

Tollgate Scenario. Let's consider a *connected vehicle case*, where driver is able to enter her personal information (e.g., Bank account info) to the car, see Fig. 3. This data is then stored in the Storage of Bank account info. When the Car approaches the Tollgate, it receives a payment request from the Tollgate. The Car sends the Payment info (i.e., the driver's name and her account number). The Tollgate processes the transaction by requesting the payment from the Bank (see Request payment). The Transaction details include driver's name, bank account, tollgate ID, and amount. The Bank performs the payment transaction and informs about its success both the Tollgate (see, Inform about successful transaction and the Driver (see, Inform about transaction). Once Tollgate receives a message about the successful transaction, it allows the Car to pass (see, Pass tollgate).

Extract AS-IS compliance model. The input for this step is the business model, which compliance should be checked, and the GDPR model, which is used to guide the extraction of the AS-IS model. The extraction includes identification of the following GDPR model elements:

Actor: The Tollgate is a *Controller*, because it "determines the purposes and means of the processing of personal data" [1]. The Tollgate is a public organisation. It does not conduct regular and systematic monitoring of data subjects (i.e., Drivers) on a large scale nor process sensitive personal data on a large scale as a core activity (see, [1] Art. 37(1)).

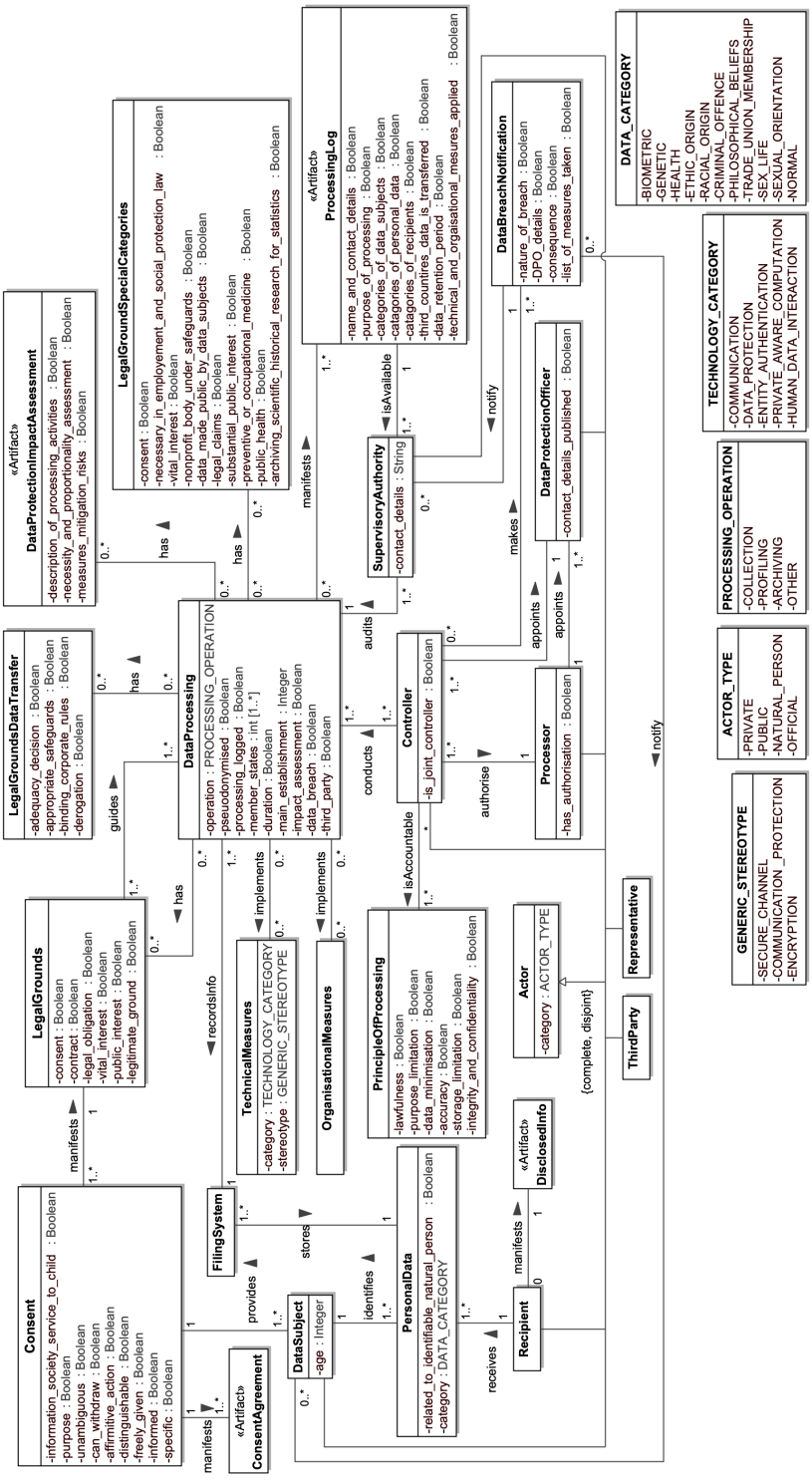

Fig. 1. GDPR model (adapted from [7][12])

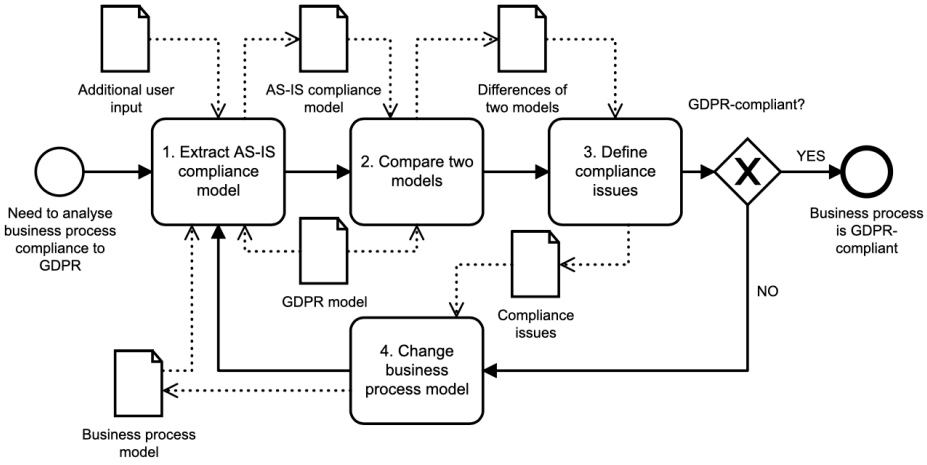

Fig. 2. Method for achieving regulation compliance, adapted from [11] [7]

Personal data and *Data subject*: As illustrated in Fig. 3, the Driver is a *Data subject* because she owns the Bank account info (i.e., *Personal data*), which could be used to identify natural person (see, [1] Art. 4(1)). The Bank account info is not sensitive personal data (category is *NORMAL*).

Filling system: The filling system is the Car (information) system, where the Driver stores her Bank account info (see Fig. 3). It is, then, accessed by the Tollgate as the Payment info (see Fig. 4) is received from the car and processed.

Processing activity: The data processing activity is Request payment. This is a data collection activity (i.e., operation = *COLLECTION*). The case does not indicate whether the payment is logged (processing_logged=*FALSE*). The Payment info is transferred to other member states (i.e., Bank) thus member_state equals to 1. There is no information about a data breach (data_breach= *FALSE*).

Records of processing: The *Tollgate* process does not include any activities to record data processing. RequestPaymentLog attributes receive *FALSE* value.

Legal grounds: The *tollgate* business process (see Fig. 3 and 4) does not indicate what legal grounds ([1] Art.6(1)) for Request payment are. The Tollgate should potentially receive the Driver's consent (see, reg. Article 6(1)(a)) for processing the Transaction details and other attributes of LegalGroundsToRequestPayment receive value *FALSE*.

Measures: The organisational (i.e., TollgateOrgMeasures) and technical (i.e., TollgateTechMeasures) measures ([1] Art. 32) cannot be read from Fig. 3 or 4.

Disclosure: As a result of the Request payment, the Bank gets the Transaction details, which include *driver name*, his *bank account*, *tollgate ID* (which could be seen as a sensitive information as it reveals driver's location) and payed *amount*.

Principle of processing: As there is no conflicting information, it is presumed that the Tollgate (as the *Controller*) follows the data processing principles (see, [1] Art. 5(1)).

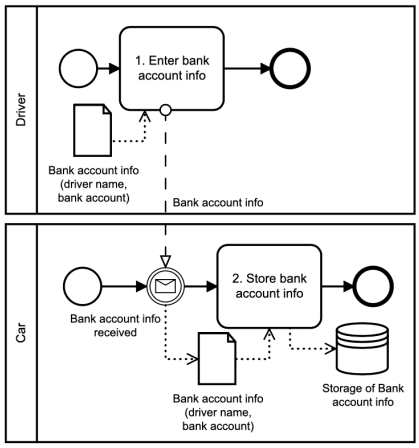

Fig. 3. Tollgate scenario: data input

Data subject rights: Let's assume that Driver wishes to rectify his Bank account info (e.g., process in Fig. 3) in the Car (see, [1] Art. 16). Fig. 5 illustrates this situation, also by covering the [1] Art. 12(3)-12(6) (i.e., identity_confirmed, action_taken_within_30_days and free_of_charge both get assigned *TRUE* value).

Compare two models and **Define compliance issues**. Table 1 presents an extract of comparison of two – the GDPR and the AS-IS – models. The instance of ProcessingLog is RequestPaymentLog. Following the [1] Art. 30(1), "each controller <...> shall maintain a record of processing activity" [1]. This is not the case in the *Tollgate* example, where logging activity is not present. Thus, the non-compliance (NC#1) issue is identified suggesting that the activity of logging needs to be introduced. The log should include the controller's name (Tollgate), purpose of processing (payment for passing the tollgate), data subject category (Driver name), personal data category (bank account info: *NORMAL*), recipient category (Bank), and the applied technical and organisational measures.

Following Art. 6(1), the processing needs to be lawful (see, correspondence between the LegalGrounds and LegalGroundsToRequestPayment) "only if and to the extent that at least one" [1] of the LegalGroundsToRequestPayment attributes receives value *TRUE*. If not, then the Consent (i.e., DriverConsent) should be given by the Data subject (i.e., Driver) "to the processing of his or her personal data for one or more specific purposes" [1]. The non-compliance issue (NC#2) is defined to indicate that the *Tollgate* case does not illustrate how the consent is given (or is there any other indications of the RequestPayment lawfulness).

Following the Art. 32(1), "the controller <...> shall implement appropriate technical and organisational measures to ensure a level of security" [1]. The TollgateOrgMeasures corresponds to OrganisationalMeasures in the GDPR model and TollgateTechMeasures – to TechnicalMeasures. However, neither TollgateOrgMeasures nor OrganisationalMeasures are defined (or visualised) in the *Tollgate* case, thus this situation results in another non-compliance issue (NC#3).

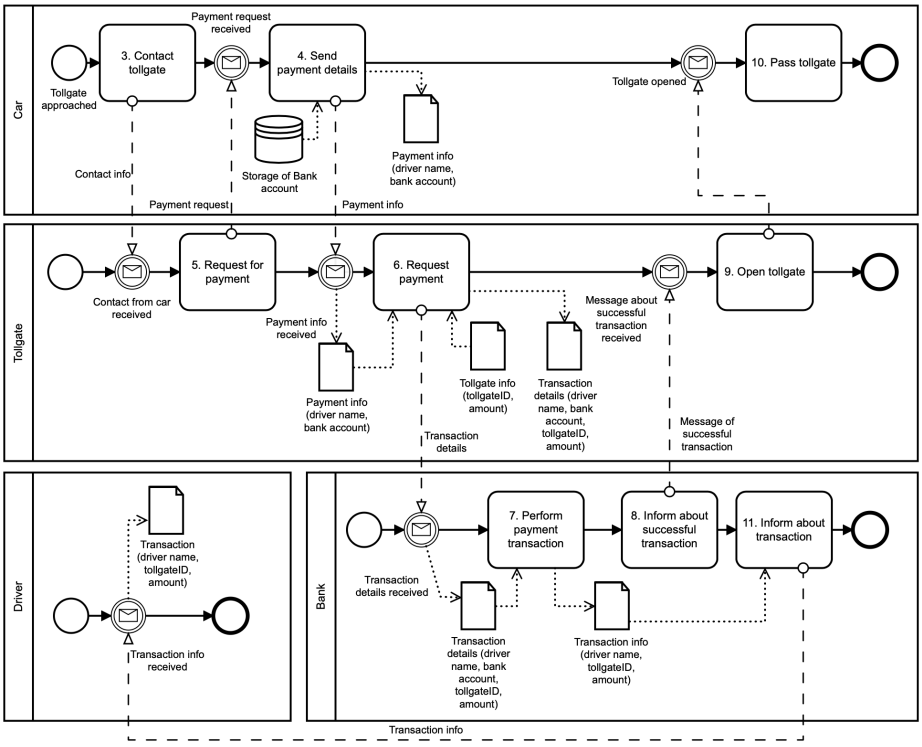

Fig. 4. Tollgate scenario: data processing

Change business process model. Fig. 6 and 7 illustrate how identified non-compliance issues are addressed in the *Tollgate* example.

NC#1: To address the first non-compliance issue, the Tollgate should contain a storage of the Logs of Request payment (see, Fig. 7). After performance of the Request payment activity, the Tollgate logs the request transaction details (see, activity C2). Besides the Transaction details, the log entry should also include the *purpose of processing*, *recipient* (i.e., Bank), *technical* (e.g., *cryptographic means*, see below) and organisational measures.

NC#2: The second non-compliance is addressed by introducing how *Driver's consent* is handled to the Tollgate. In Fig. 6, while entering the Bank account details, the driver should also Provide the consent to process Bank account details (see activity *C1.2*). The consent is then placed in the storage contained in the Car (information system). When processing the Payment info (see, Fig. 7), the Tollgate checks the driver's consent validity (see, activity *C1.4*). If it is not valid, the Tollgate informs driver about the invalid consent (see, activity C1.5), otherwise it proceeds with the data processing activity (see, Request payment).

NC#3: In the *tollgate* example we discuss one set of technical measures. In Fig. 6, activity *C3.1* illustrates that the Bank account info should be encrypted.

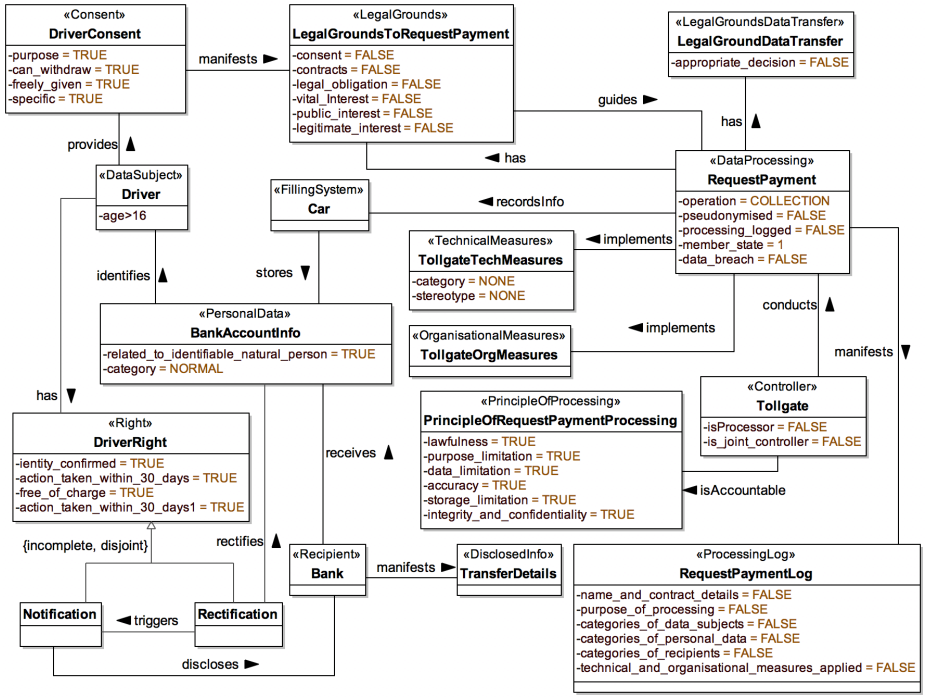

Fig. 5. Tollgate scenario: AS-IS Compliance Model

The encrypted data are stored in the Car (information system). Then, in Fig. 7, the Tollgate receives it from the Car (see, Payment info) and submits it to the Bank (see, Transaction details). The Bank uses the Private key to decrypt the Bank account info in order to perform the payment transaction.

5 Discussion and Concluding Remarks

Tool support. To support the GDPR compliance method (see Section 4), a prototype tool (see, *https://github.com/motekaj/gdpr-analyzer*) [11] is implemented. The main functions of the prototype support the method for achieving

Table 1. Table captions should be placed above the tables.

Reg. Article	GDPR model	AS-IS compliance model	Non-compliance issue
30(1)	ProcessingLog	RequestPaymentLog	NC#1
6(1)	LegalGrounds	LegalGroundsToRequestPayment	NC#2
6(1)	Consent	DriverConsent	NC#2
32(1)	OrganisationMeasures	TollgateOrgMeasure	NC#3
32(1)	TechnicalMeasures	TollgateTechMeasure	NC#3

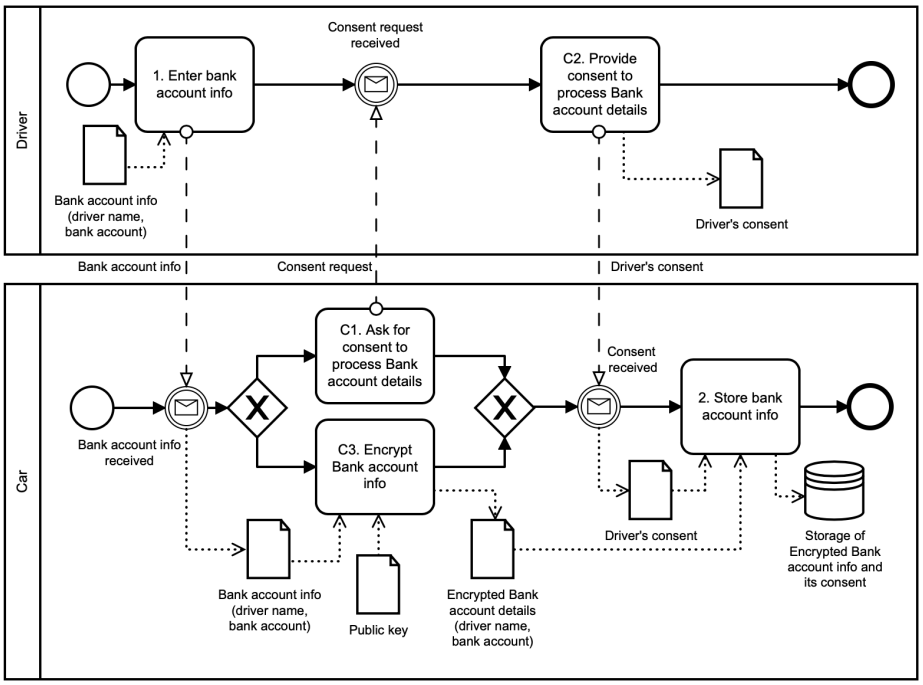

Fig. 6. Tollgate scenario: non-compliance resolution for data input

regulation compliance (see, Fig. 2) and include (step 1) extraction of the AS-IS compliance model, (step 2) comparison of the two models, and (step 3) definition of compliance issues. The tool helps to detect the non-compliance issues as *flags* attached to the relevant model elements and lists the recommended guidelines to address them in the business process model. The updated model should be the input to the next iteration of the compliance checking (i.e., step 1 of the method).

Limitation. The GDPR model does not consider how it may be adapted in a national context. The GDPR leaves a room for Member States to deviate on some aspects (including the legal grounds of processing that may arise from the national laws). The model would have to be adjusted when there are aspects that controller must take into account to achieve compliance.

Completeness of the GDPR model. The GDPR regulation includes 99 articles (including 191 (sub)articles in total), but not all articles consider specific legal requirements for organisations. Some articles contain generic effort clauses that are not fit for modelling. The model given in Fig. 1 addresses only the specific[6] legal requirements obliging controllers and processors. In addition the GDPR model includes several special cases concerning the applicability criteria

[6] The ones, which can be represented using UML activity, association or class notations.

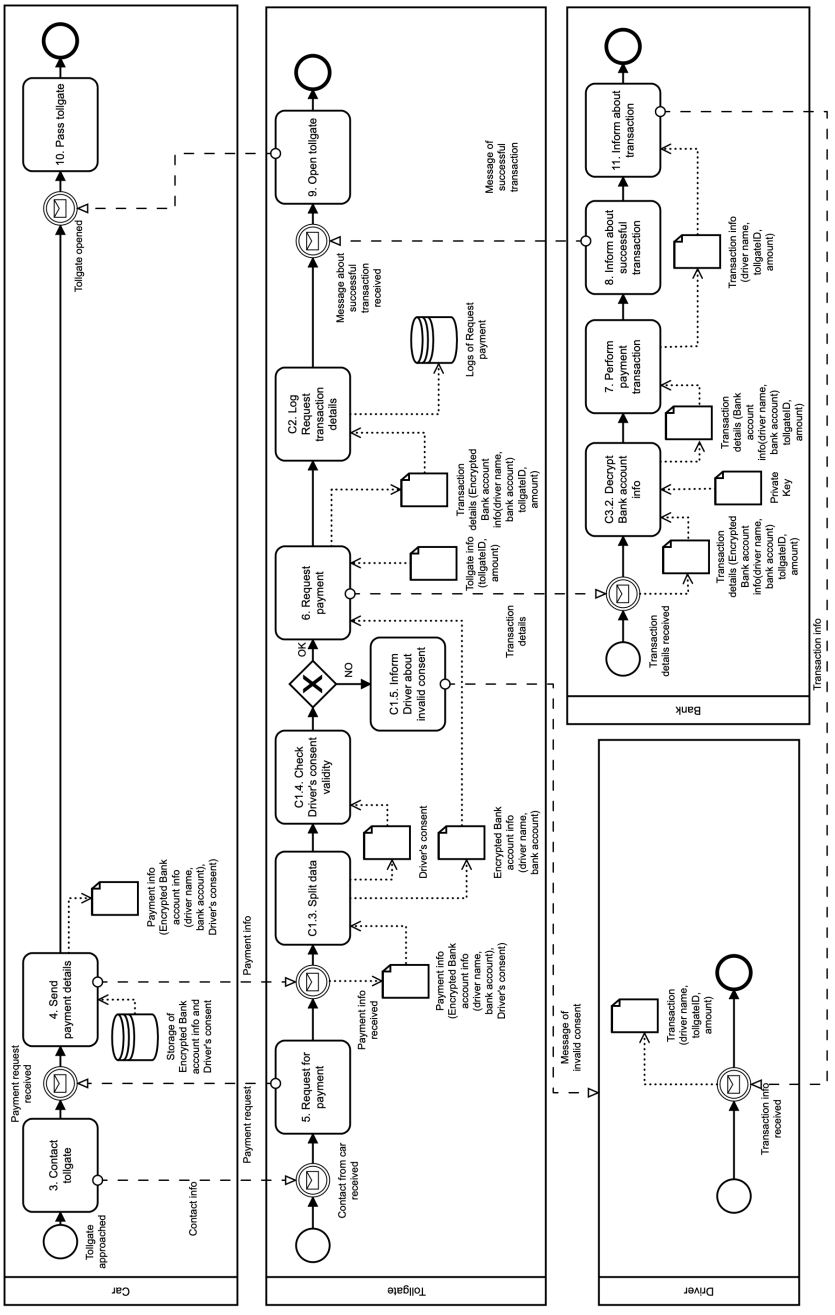

Fig. 7. Tollgate scenario: non-compliance resolution for data processing

which are presented using the BPMN notations in [7]. The additional applicability criteria are (*i*) conducting a data protection impact assessment or prior consultation with the supervisory authority [1] Art. 35 and 36; (*ii*) processing of special categories of data on a legal basis [1] Art. 9(2); (*iii*) transferring personal data to a third country [1] Art. 45(1), 46(1), 46(2), 46(3), 47(1) and 49(1); (*iv*) making a data breach notification in case of a data breach [1] Art. 33 and 34.

In total the GDPR model (see details in [7]) concerns 40 articles (including 75 (sub)articles) resulting in rather high completeness (in comparison to other works [9] [4] [13]) while checking the compliance of the business processes.

Administrative fines. Organisations want to be compliant in order to avoid administrative fines. Non-compliance of the data processing principles is a main infringement under [1] Art. 83(5)(a). The GDPR model includes analysis of *legal ground*, *legal ground special categories* and *legal ground data transfer*, which guides the *data processing*. The *legal ground special category* and *legal ground data transfer* define the legality of processing special data categories [1] Art.9(2)] and the legality of data transfers to third countries. The model includes all the *data subject rights* which cover [1] Art. 12(3)-12(6) and helps avoiding fines.

The *data processing* and *accountability* principles [1] Art. 5] are included, too. The obligation to conduct a *data protection impact assessment* and *prior consultation* enable the organisation to decide whether these needs to be conducted and if so, what are the content requirements. The *data processing* also includes three attributes for *impact assessment*, [1] Art. 33-35, *data breach* [1] Art. 45(1), 46(1), 46(3), 47(1) and *third country* [1] Art. 49(1). Besides the *technical measures*, the GDPR model also considers the *organisational measures* [1] Art. 32(1), 25(1) and 25(2)]. Addressing these compliance issues minimises the risk of incurring administrative fines.

Validity. In addition to the *tollgate* scenario, the GDPR model, its supporting method and tool have been applied in a few other cases. In [5], the GDPR model is used to support modelling of the goal-actor-rule perspective. The study shows how modelling language could be extended to capture infringement and to solve it using embodiment, finding irregularities, compliance checking and irregularity resolution activities. In [2] the GDPR model is applied in an airline contact centre processes. The results of both cases ([5] and [2]) were introduced to the domain experts who found the application of the GDPR model intuitive and helpful to achieve business process compliance.

In [11] the manual application of the method to achieve regulation compliance is compared to the tool-supported analysis. The results indicate a high correspondence between the number of found non-compliance issues. In addition the tool-supported application is able to highlight non-compliance issues (e.g., application of the technical measures), which were omitted from the manual analysis.

Future work. Both, the GDPR model and method for achieving compliance needs further refinement. Future research is also needed for tool support regarding the *change of the business process model* (see Step 4, Fig. 2). Potentially, *process design patterns* [3] could be useful, but one needs to define the

link between the identified non-compliance issues and the available patterns.

Acknowledgement. This paper is supported in part by European Union's Horizon 2020 research and innovation programme under grant agreement No 830892, project SPARTA. We would like also to thank Manon Knockaert (*University of Namur*) for the constructive comments while preparing this paper.

References

1. EU General Data Protection Regulation, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L .2016.119.01.0001.01.ENG
2. Abbasi, A.: GDPR Implementation in an Airline Contact Center. Master's thesis, University of Tartu (2018)
3. Agostinelli, S., Maggi, F.M., Marrella, A., Sapio, F.: Achieving GDPR Compliance of BPMN Process Models. In: Information Systems Engineering in Responsible Information Systems. CAiSE 2019. LNBIP, vol. 350, pp. 10–22 (2019)
4. Blanco-Lainé, G., Sottet, J.S., Dupuy-Chessa, S.: Using an Enterprise Architecture Model for GDPR Compliance Principles. In: The Practice of Enterprise Modeling. pp. 199–214. Springer, Cham (2019)
5. Çelebi, I.: Privacy Enhanced Secure Tropos: A Privacy Modeling Language for GDPR Compliance. Master's thesis, University of Tartu (2018)
6. C'M'S': GDPR Enforcement Tracker, https://enforcementtracker.com/
7. Kala, K.: Refinement of the General Data Protection Regulation (GDPR) Model: Administrative Fines Perspective. Master's thesis, University of Tartu (2019)
8. Mammüller, F., Ogunyawo, P., Probst, C.: Designing Data Protection for GDPR Compliance into IoT Healthcare Systems
9. Pandit, H.J., Polleres, A., Bos, B., Brennan, R., Bruegger, B., Ekaputra, F.J., Fernández, J.D., Hamed, R.G., Kiesling, E., Lizar, M., Schlehahn, E., Steyskal, S., Wenning, R.: Creating a Vocabulary for Data Privacy. In: On the Move to Meaningful Internet Systems: OTM 2019 Conferences. pp. 714–730. Springer (2019)
10. Pullonen, P., Tom, J., Matulevičius, R., Toots, A.: Privacy-Enhanced BPMN: Enabling Data Privacy Analysis in Business Processes Models. Software and Systems Modeling **18**(6), 3235–3264 (Dec 2019)
11. Sing, E.: Meta-Model Driven Method for Establishing Business Process Compliance to GDPR. Master's thesis, University of Tartu (2018)
12. Tom, J., Sing, E., Matulevičius, R.: Conceptual Representation of the GDPR: Model and Application Directions. In: Perspectives in Business Informatics Research. BIR 2018. vol. 330. Springer (2018)
13. Torre, D., Soltana, G., Sabetzadeh, M., Briand, L.C., Auffinger, Y., Goes, P.: Using Models to Enable Compliance Checking against the GDPR: An Experience Report. In: Proceedings of the 22nd International Conference on Model Driven Engineering Languages and Systems (MODELS 19) (2019)