Managing Consent in Workflows under GDPR

Saliha Irem Besik and Johann-Christoph Freytag

Humboldt-Universität zu Berlin, Department of Computer Science,
Unter den Linden 6, 10099 Berlin, Germany
{besiksal,freytag}@informatik.hu-berlin.de

Abstract. The European Union General Data Protection Regulation (GDPR) defines the principles to be met by organizations when processing personal data in order to guarantee data privacy. According to GDPR, consent is required for establishing a legal basis for processing personal data, if there are no other legal grounds for the processing. Besides any identifiable "natural" person, also known as data subject, has the right to withdraw the given consent to process his or her personal data at any time. It is the organization's responsibility to ensure consent and its revocation to demonstrate its compliance with GDPR. With respect to GDPR compliance, organizations can benefit from workflows as they might be used to ensure that consent is obtained before processing personal data. This paper addresses how to enable organizations to manage consent and revocation through their workflows.

Keywords: Data Privacy · General Data Protection Regulation (GDPR) · Consent · BPMN · Business Process Compliance

1 Introduction

The European Union General Data Protection Regulation (GDPR) limits the processing personal data unless it is explicitly allowed by law, or the data subject has consented to the processing [GDPR, Article 6]. In addition to this, the data subject shall have the right to withdraw his or her consent at any time [GDPR, Article 7(3)]. Organizations dealing with personal data of European Union citizens must be able to provide a proof of validity of obtained consent and revocation.

The principle of Privacy by Design (PbD) advocates that privacy should be considered as a first class citizen in the technology design and should be proactively embedded. In order to support PbD, organizations can take advantage of workflows by checking compliance of their workflow models with GDPR during design time. One of the significant benefits of using workflows is that it enables to capture how data is transmitted for what purpose at the conceptual level. We use Business Process Model and Notation (BPMN) to model workflows as it is a de-facto standard for business process modeling.

In this paper, we analyze the consent and its revocation under GDPR. Based on this analysis, we propose design patterns to integrate consent and revocation features in BPMN-based workflows.

J. Manner, S. Haarmann, S. Kolb, O. Kopp (Eds.): 12th ZEUS Workshop, ZEUS 2020, Potsdam, Germany, 20-21 February 2020, published at http://ceur-ws.org/Vol-2575

The structure of the rest of the paper is as follows: Section 2 briefly presents our understanding of the consent and revocation under GDPR. Section 3 discusses the concept of workflows in our research. Section 4 gives an overview of our proposed approach. Section 5 gives a running example in the clinical domain to show the applicability of our approach. Section 6 reviews related works. Finally, Section 7 concludes this paper and discusses our future work and perspectives.

2 Consent and Revocation under GDPR

Consent can be defined as "any freely given, specific, informed and unambiguous [...] clear affirmative action" by which a data subject agrees to the processing of his or her personal data [GDPR, Article 4]. Some data operations are lawful only if the data subject has given consent to this processing [GDPR, Article 6, §1(a)].

Organizations need to determine whether their data operations require consent to be lawful. We use the term *Consent Policy* to define the statements to declare whether a data operation requires a consent. In our article [1], we gave a formal definition for *Consent Policy* in Definition 1.

Definition 1 (Consent Policy) *A Consent Policy CP contains policies which are represented as 2-tuples cp = (purpose, requiresConsent), where:*

- *purpose is the reason for which data is collected, used, or disclosed;*
- *requiresConsent* $\in \{true, false\}$ *specifies whether data processing requires consent or not.*

For instance, newborn hearing screening requires an explicit consent to be legitimate. However, an emergency case does not require consent as it is a subject of "vital interest" which means being necessary to protect someone's life. Thus, CP contains policies *(newborn-hearing-screening, true)* and *(vital-interest, false)* accordingly.

For consent to be informed and valid, the data subject must be aware at least of the purposes of the processing and the identity of the data controller who determines the purposes and means of the processing [GDPR, Recital 42]. As an example, assume Hospital X wants to use personal data of its patients for newborn hearing screening. Hospital X can use the following statement to inform its patients to obtain consent *"We, as Hospital X, use your personal data for the purpose of newborn hearing screening."*

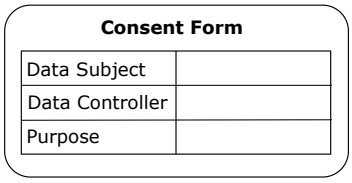

Fig. 1. Consent Form.

We modeled *Consent Form* (illustrated in Figure 1) that retains the minimum required information to be valid. *Consent Form* can be elaborated with additional information such as the duration of the consent to give data subjects more control.

A data subject has the right to withdraw his or her consent at any time [GDPR, Article 7, §3]. Organizations are obliged to take appropriate actions to handle revocation. They have to stop any ongoing process instances which are affected by revocation. They should also delete the personal data, if the personal data is not used by any other purpose and becomes unnecessary after revocation.

3 Workflows: Platform to support GDPR Compliance

Data privacy, in general, focuses on how personal data should be handled. In order to ensure data privacy in BPMN-based workflows, we worked on different ways of data handling supported in BPMN [2]. Data is represented in BPMN via data object, data store, or message elements[1] (shown in the left-hand side of Figure 2). In order to check the privacy compliance of a workflow, for each of its data operations it is essential to know explicitly which personal data is accessed for which purpose. We expect organizations to provide this information via semantic text annotations. Right-hand side of Figure 2 illustrates how we semantically annotate the data operations, where *purpose* refers to the purpose of accessing data and *attribute-name* refers to a set of attribute names of data which are accessed. For example, $< marketing, \{name, age\} >$ annotation means *name* and *age* data attributes are accessed for the purpose of *marketing*.

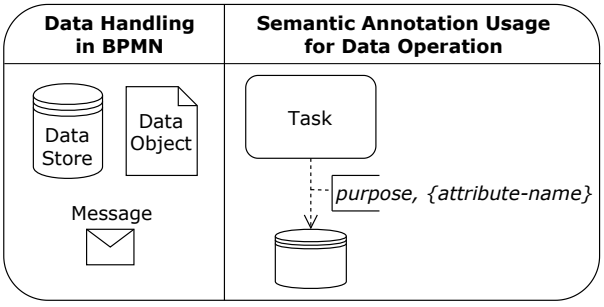

Fig. 2. Data in BPMN.

4 Approach

Our idea how to manage consent and revocation is to propose design patterns that are integrated into BPMN-based workflows. As we explained in Section 2, some data operations are legitimate only with the consent of a data subject. As a first step, we determine the data operations in a given workflow. Section 3

[1] https://www.omg.org/spec/BPMN/2.0/

lists different means to handle data in BPMN which are via data object, data store, or message elements. We check these BPMN elements in a given workflow. We assume that data operations are all semantically annotated and semantic annotations include the purpose of the data operations.

After finding each data operation in a given workflow, we determine whether these data operations require consent according to a given *Consent Policy* (Definition 1). If there is a data operation requiring explicit consent and if there is no consent obtained before that data operation, there is a potential privacy violation. Our idea is adding a checking consent step beforehand to remove this potential violation. For this purpose, we designed a consent pattern which is shown in Figure 3. *Data Controller* asks the *Data Subject* for consent and the *Data Operation* is executed when consent is granted. Otherwise, the process terminates. *Consent Form* is modeled as it is shown in Figure 1, it contains the identity of *Data Controller* and the purpose of the *Data Operation*.

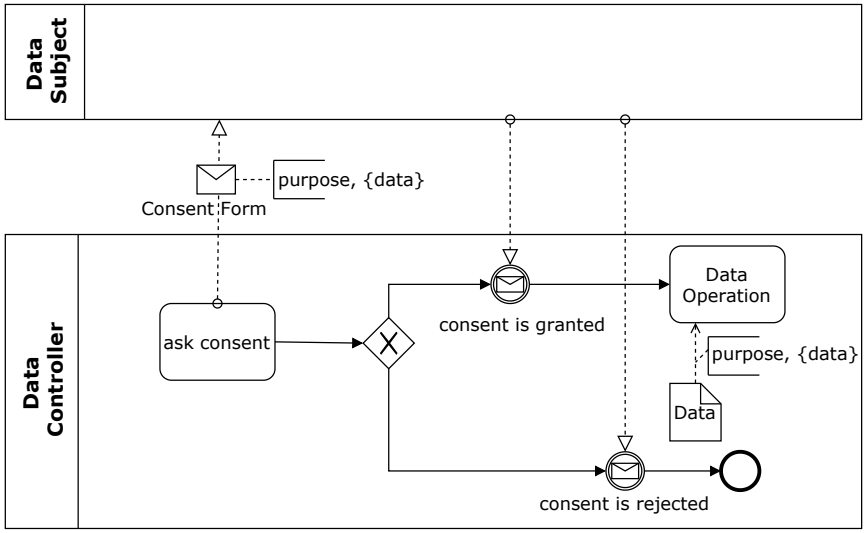

Fig. 3. Consent Pattern.

We address the question "when to obtain consent?" Our idea is to add consent pattern as late as possible which means adding it just before the concerned data operation. In this way, we intend to prevent the potential situations where consent is obtained yet never used. We argue that consent should be obtained only when it is needed. We raise also the question "what if there are multiple purposes within a given workflow?" When there are multiple purposes, consent should be given for all of them [GDPR, Recital 42]. Our strategy to handle multiple purposes is first checking whether the data operations with different purposes

always follow each other. When they always follow each other, we create one aggregated *Consent Form* including all their purposes. If data operations do not always occur together, we create separate consent patterns for each of these data operations. The reason behind is again related to prevent the potential situations where consent is obtained yet never used. Creating separate consent patterns might increase the complexity of the workflows in terms of readability. However, a consent pattern can also be designed as a collapsed BPMN sub-process which provides a more compact view. Thus, we might increase the readability of the workflow.

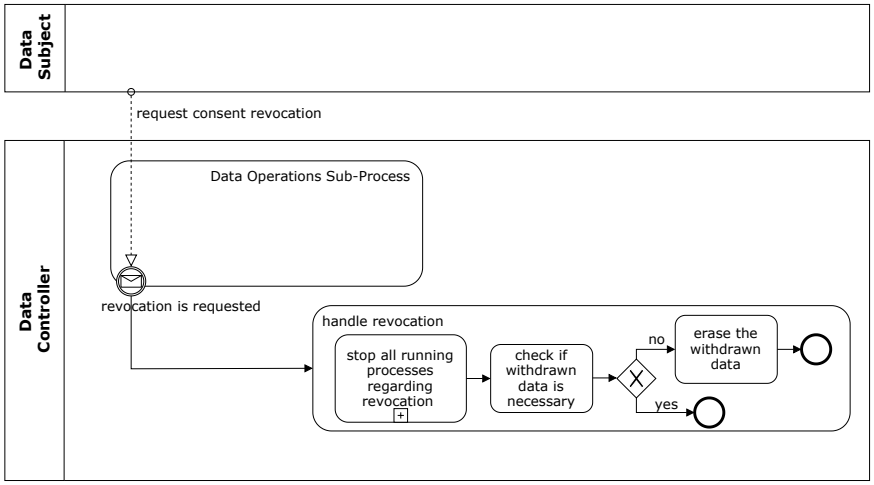

Fig. 4. Revocation Pattern.

Figure 4 shows our design pattern to handle revocation. We create a sub-process which includes all data operations because the consent withdrawal can be related to any of the data operations. We also add a *"handle revocation"* step for the created sub-process. *Handle revocation* task is triggered by withdrawal request by a data subject. Handling revocation implies to stop any ongoing process instances affected by the withdrawal request of the data subject and to erase the personal data if the personal data is not necessary anymore.

We developed both consent and revocation patterns in a way that no additional BPMN symbol is required. In this way, our approach can be easily applied to existing BPMN-based workflows.

5 Running Example

We consider Newborn Hearing Screening (NHS) procedure in Germany as a running scenario in order to illustrate our methodology. It is an optional procedure

which requires the explicit consent of at least one of the parents or guardians of the newborn babies. After carrying out NHS, according to the result of the screening pediatrician either applies treatment or conducts further research. Processing personal data for the purpose of research also requires consent to be lawful. Figure 5 shows a BPMN diagram for our scenario. Take note that this BPMN diagram is not GDPR-aware which means there is neither consent nor revocation control.

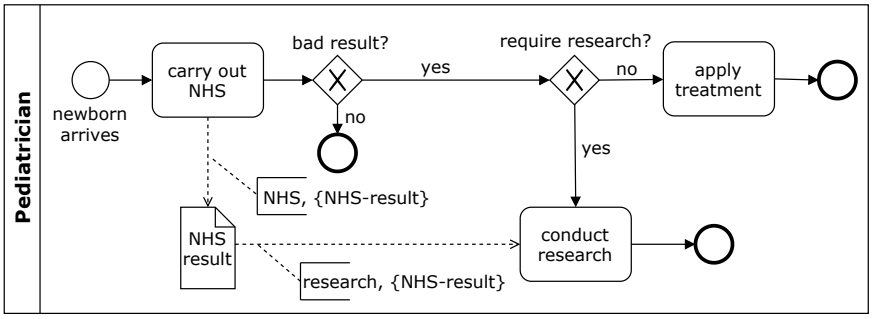

Fig. 5. Newborn Hearing Screening Diagram without Consent and Revocation.

Figure 6 illustrates the BPMN diagram for newborn hearing screening which includes consent and revocation controls.

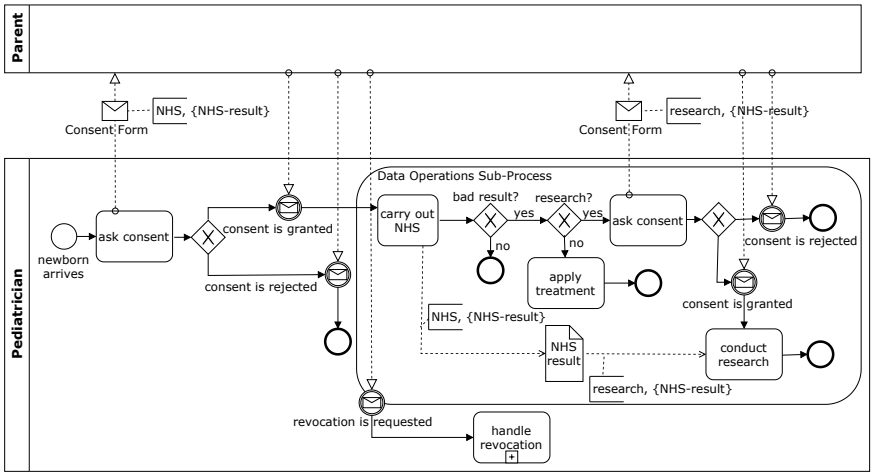

Fig. 6. Newborn Hearing Screening Diagram with Consent and Revocation.

In our scenario, there are two data operations with two different purposes which are NHS and research. We add separate consent patterns for each of these data operations because when the processing has multiple purposes, consent should be given for all of them. In our scenario, pediatrician do not always conduct research. Therefore, we do not ask consent for research and NHS at the same time. In order to manage revocation, we create the *Data Operations Sub-Process* including both data operations and we add handle revocation pattern for this sub-process. *Handle revocation* task is triggered by a revocation request by a parent.

6 Related Work

Granting and revoking consent effectively has been the focus of several research efforts over the last years. In the pre-GDPR era, one of the pioneers in this field is Ensuring Consent and Revocation (EnCoRe) research project. Within this project, one of the goals was to provide dynamic and granular options for consent and revocation in system design [3][4]. They also provided conceptual modeling for privacy policies with consent and revocation requirements [5]. Their understanding of consent differs from ours as they do not reflect on the requirements and obligations based on GDPR. Also, they have no work regarding the use of workflows to handle consent and revocation. [6] proposed the idea of the alignment of workflows with consent management. Their aim was, however, generating the letter of consent documents based on existing workflows. In the literature, there are also studies where BPMN is extended towards security and privacy aspects [7][8]. However, these works do cover neither consent nor revocation. [9] presented a set of design patterns as business process models which enables organizations to tackle GDPR constraints. Their work can be considered as a guide to achieve GDPR compliance for an organization. Our work considerably differs from their work because we aim to transform the existing non-privacy-aware business process models into privacy-aware ones.

7 Conclusion and Outlook

We are convinced that it is fundamental to incorporate consent and revocation controls within the workflows of organizations that handle personal data to ensure their compliance with GDPR during the design time. In this paper, we presented our approach to adapt the BPMN-based workflows with the consent and revocation concepts under GDPR. As future work, we would like to work on how to automatically generate the consent forms by using the existing workflows and automatically transform the existing workflows into the ones which handle the consent and revocation efficiently. We are also interested in analyzing the optimality of our approach.

References

1. Saliha Irem Besik and Johann-Christoph Freytag. A formal approach to build privacy-awareness into clinical workflows. *SICS Software-Intensive Cyber-Physical Systems*, pages 1–12, 2019.
2. Saliha Irem Besik and Johann-Christoph Freytag. Ontology-based privacy compliance checking for clinical workflows. In *Proceedings of the Conference on "Lernen, Wissen, Daten, Analysen", Berlin, Germany, September 30 - October 2, 2019*, pages 218–229, 2019.
3. Marco Casassa Mont, Siani Pearson, Gina Kounga, Yun Shen, and Pete Bramhall. On the management of consent and revocation in enterprises: setting the context. *HP Laboratories, Technical Report HPL-2009-49*, 11, 2009.
4. Ioannis Agrafiotis, Sadie Creese, Michael Goldsmith, and Nick Papanikolaou. Reaching for informed revocation: Shutting off the tap on personal data. In *IFIP PrimeLife International Summer School on Privacy and Identity Management for Life*, pages 246–258. Springer, 2009.
5. Marco Casassa Mont, Siani Pearson, Sadie Creese, Michael Goldsmith, and Nick Papanikolaou. A conceptual model for privacy policies with consent and revocation requirements. In *IFIP PrimeLife International Summer School on Privacy and Identity Management for Life*, pages 258–270. Springer, 2010.
6. Nils Gruschka and Meiko Jensen. Aligning user consent management and service process modeling. In *GI-Jahrestagung*, pages 527–538, 2014.
7. Wadha Labda, Nikolay Mehandjiev, and Pedro Sampaio. Modeling of privacy-aware business processes in BPMN to protect personal data. In *Proc. of the 29th Annual ACM Symposium on Applied Computing*, pages 1399–1405. ACM, 2014.
8. Alfonso Rodríguez, Eduardo Fernández-Medina, and Mario Piattini. A BPMN extension for the modeling of security requirements in business processes. *IEICE transactions on information and systems*, 90(4):745–752, 2007.
9. Simone Agostinelli, Fabrizio Maria Maggi, Andrea Marrella, and Francesco Sapio. Achieving gdpr compliance of bpmn process models. In *International Conference on Advanced Information Systems Engineering*, pages 10–22. Springer, 2019.