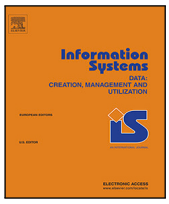
Information Systems 137 (2026) 102646

Contents lists available at ScienceDirect

Information Systems

journal homepage: www.elsevier.com/locate/is



Design patterns for GDPR-aware process modeling in BPMN

Simone Agostinelli [a,*], Francesca De Luzi [b], Fabrizio Maria Maggi [c], Andrea Marrella [b], Alessia Volpi [b]

[a] Mercatorum University of Rome, Piazza Mattei 10, 00186, Rome, Italy
[b] Sapienza University of Rome, via Ariosto 25, 00185, Rome, Italy
[c] Free University of Bozen-Bolzano, Piazza Domenicani 3, 39100 Bolzano, Italy

ARTICLE INFO

Keywords:
Data privacy by design
GDPR
Design patterns
Business processes
Process models
BPMN

ABSTRACT

In an increasingly digital world, collecting, processing, and exchanging personal data are critical drivers for enacting enterprise business processes. However, the long-term retention and access of personal data expose organizations to data breaches, in which sensitive and protected data are disclosed and exploited unauthorizedly. To mitigate the damage that data breaches can cause, in the European Union (EU), the right to data privacy is enforced through the General Data Protection Regulation (GDPR), which defines how organizations must store and manage EU citizens' data. GDPR is highly influencing how organizations approach data privacy, forcing them to rethink and upgrade their business processes to become GDPR compliant, which can be daunting. In this paper, in line with the privacy-by-design principles of GDPR, we propose a methodology that shows how to capture the main privacy GDPR constraints in the form of design patterns and integrate them into business process models specified in BPMN (Business Process Model and Notation). This allows us to achieve full transparency of privacy constraints in business processes, making it possible to ensure their compliance with GDPR at design-time. We adopt a design science research approach to present our methodology and make design decisions explicit. We also introduce GDPR-Pilot, a BPMN editor that assists process designers and Data Controllers in integrating GDPR patterns into existing models. The methodology is evaluated through real-world use cases against structural, usage, and environmental requirements.

1. Introduction

Nowadays, the increase in both storage and processing power has made it possible to virtually store and process all the information that might be relevant for an organization to rapidly deliver digital and physical services to their customers (e.g., the creation of a bank account, the management of a purchase order, etc.). In this context, the seemingly never-ending collection of customers' data by large corporations has raised public awareness of privacy concerns [1]. Moreover, with the rise of Large Language Models (LLMs), the debate around the unauthorized use of personal data to train the LLMs has forced some European (EU) countries to issue a temporary ban in 2023 on such technologies due to the legal uncertainty regarding the data privacy and data ownership compliance.[1]

Since 25 May 2018, the General Data Protection Regulation (GDPR) tackled in the EU the *right to privacy* for personal data, intending to protect EU citizens from privacy breaches.[2] Since non-compliance with the GDPR can result in heavy fines, organizations must correctly implement GDPR data management policies and take appropriate action on customer data upon request. Among the various technical and non-technical challenges to achieving GDPR compliance [2], the regulation enforces organizations to reshape the way they approach the management of personal data stored and exchanged during the execution of their business processes [3]. A business process is a collection of activities aimed at delivering a product or service to a customer while fulfilling an organizational goal [4]. Business processes are typically specified using dedicated languages such as BPMN[3] (Business Process Modeling and Notation), which is considered the de facto standard for process modeling, due to its intuitive graphical notation and wide support among commercial Business Process Management Systems (BPMSs) [5].

Although BPMN is well-suited for modeling stakeholder collaboration and data flow between business process activities [6], making it a

* Corresponding author.
E-mail address: simone.agostinelli@unimercatorum.it (S. Agostinelli).

[1] https://www.edpb.europa.eu/system/files/2024-04/edpb_annual_report_2023_en.pdf
[2] https://www.consilium.europa.eu/en/policies/data-protection-regulation/
[3] http://www.omg.org/spec/BPMN/2.0/

https://doi.org/10.1016/j.is.2025.102646
Received 26 January 2024; Received in revised form 2 November 2025; Accepted 12 November 2025
Available online 14 November 2025

potentially effective tool for identifying privacy breaches before business process execution, its use for systematic privacy analysis at design-time remains limited [7]. Conversely, organizations tend to rely on non-automated solutions for regulatory compliance, resulting in costly manual implementation and audits to ensure GDPR adherence [8]. Consequently, the common practice to address privacy breaches in a business process is to implement ad-hoc countermeasures (e.g., in the form of scripts or business rules) during the automation stage of the process life-cycle, when the process model is configured by a system engineer (SE) for its execution with a BPMS [4,9,10]. However, this approach requires that the SE knows precisely where potential privacy breaches can manifest in the business process. This information, if not explicitly documented in the process model, may lead to a defective implementation of compensatory strategies from privacy breaches. Since BPMN can explicitly mark the data artifacts involved in a business process, we can directly pinpoint the privacy issues that the process might suffer within the process model. While many literature works (e.g., [6–8,10–20]) explicitly extend BPMN with cyber-security and privacy requirements expressed through novel constructs, such extensions are not readily perceived by business analysts, who are the primary users of process models and, more importantly, cannot be processed by commercial BPMSs, which only accept models fully compliant with the BPMN standard.

Building on the above, and assuming a syntactically correct BPMN model, this paper presents a methodology for capturing the main GDPR privacy constraints as design patterns and integrating them into BPMN models without modifying or extending the notation. The approach promotes privacy awareness at design-time, enabling process designers to analyze the data involved and proactively prevent potential privacy violations by mitigating their impact. Our solution is intended for process designers and Data Controllers as primary users for such process models, who are responsible for: (i) modeling the activity sequences of the business process in BPMN; (ii) identifying vulnerabilities, and (iii) adopting appropriate countermeasures. Furthermore, we handle standard BPMN descriptions that can be readily implemented via customary BPMN technologies, such as the commercial BPMSs.

We structure the paper following the activities outlined in [21] for delivering a design science artifact (Section 2). After providing a detailed background analysis of the GDPR, we present the results of a dedicated survey with 33 GDPR experts, from which we identified two research challenges to achieve GDPR compliance at design-time (Section 3). Next, Section 4 situates our methodology within the state of the art, after which we define the requirements guiding the modeling of our solution (Section 5). This includes a brief introduction to BPMN and the presentation of a motivating use case related to the SIM activation process of a phone company, which serves as the running example throughout the paper. Two additional use cases, related to a hiring process and a healthcare procedure, are presented in the appendix for space reasons, although they are used in the evaluation of the methodology. In Section 6, we present the design and development of our methodology, which is grounded in nine design patterns that embed privacy-enhancing features into BPMN models in line with the GDPR. We then provide guidance on the appropriate application of each pattern and illustrate the software architecture of GDPR-Pilot, a BPMN editor developed to semi-automatically assist process designers in applying our methodology and integrating the GDPR patterns in an existing BPMN model. In Section 7, we demonstrate the *feasibility* of our methodology through the proposed use cases, evaluating it against structural (*modularity*), usage (*comprehensibility*, *customizability*, and *learnability*), and general environmental (*correctness*) requirements. The evaluation was performed in two steps. First, a preliminary assessment was conducted with 67 MsC students of Management Engineering and Computer Science Engineering familiar with BPMN, who were asked to transform a non-GDPR-compliant BPMN model into a compliant version by applying the methodology without the support of GDPR-Pilot. Second, we carried out an evaluation using GDPR-Pilot. In this phase, 21 process analysts from the three application domains of our use cases were asked to analyze the corresponding processes and apply the methodology to transform them in GDPR-compliant models. We also assessed the usability of GDPR-Pilot using the well-established System Usability Scale (SUS) questionnaire [22]. Finally, in Section 8 we draw conclusions, outline limitations and trace future work.

This paper extends our previous work [9] in several directions, incorporating new elements that were previously unexplored. Specifically, (i) we explicitly describe and discuss the design-science research approach used to systematically develop our methodology; (ii) we present the results of a dedicated survey conducted to derive the research questions guiding this study; (iii) we introduce two novel use cases to evaluate the methodology; (iv) we model two additional GDPR patterns (*Right to Object to Automated Processing* and *Right to Restrict Processing*) and specify them in BPMN; (v) we formalize the logic for systematically deciding when a design pattern should be introduced into a process model to ensure GDPR compliance; (vi) we develop a dedicated software tool (GDPR-Pilot) to support the application of the methodology; (vii) we demonstrate and evaluate our methodology with two different user groups, both without and with the use of the tool; (viii) we revise and expand the background and related work necessary to contextualize the paper.

2. Research approach

As mentioned in the Introduction, our research approach is inspired by the Design Science principles outlined by [21], and it is applied through four sequential phases as shown in Fig. 1: (1) Problem Explication, (2) Requirements and Use Case Definition, (3) Design and Development, and (4) Demonstration and Evaluation. In the following, we briefly describe the implementation of this approach.

(1) Problem Explication. This phase, which is addressed in Section 3, has a twofold objective. First, we outline the problem being tackled by analyzing the main GDPR features (i.e., the entities involved, the definition of personal data, and the obligations of the Data Controller, presented as a list of privacy constraints to be respected). Then, we present the survey results conducted with 33 GDPR experts to derive the research questions guiding the specification of the main privacy GDPR constraints in business processes at design-time. The amount of research literature on this topic further underscores the relevance of the problem, as discussed in Section 4.

(2) Requirements and Use Case Definition. The second phase, detailed in Section 5, focuses on defining the requirements addressed by our research solution. According to [21], a design science artifact should be designed and evaluated through structural, usage, management, and generic environmental requirements. As no relevant factors were identified for management requirements in our context, they are excluded from consideration. This section also introduces the main BPMN concepts and modeling constructs necessary to specify and apply GDPR-related design patterns. Finally, we present a use case involving personal data, which serves as a running example to demonstrate the feasibility of our pattern-based approach. Due to space constraints, two additional use cases employed to evaluate our solution against the defined requirements are provided in the appendix.

(3) Design and Development. The third phase concerns the creation of the design science artifact. In Section 6 we show how we modeled our solution using BPMN, and motivate the rationale behind our design decisions. The result consists of a list of nine GDPR privacy patterns for BPMN, which represent actionable, design-time strategies for addressing privacy constraints in business process models. In addition, we provide guidance on when each pattern should be applied and we introduce GDPR-Pilot, a BPMN editor developed to semi-automatically

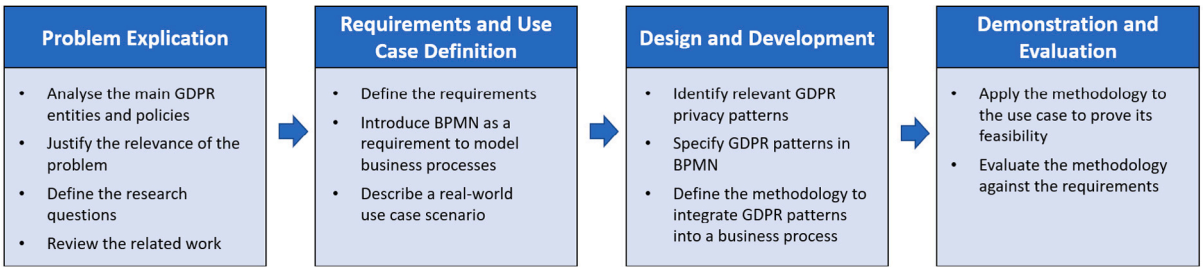


Fig. 1. Research approach based on Design Science principles by [21].

support process designers in implementing our solution and integrating the patterns into existing BPMN models.

(4) Demonstration and Evaluation. The fourth phase, discussed in Section 7, first applies the artifact, i.e., demonstrates its feasibility by applying the GDPR privacy patterns to the use case of the running example. Then, it evaluates the artifact's effectiveness in addressing the identified problem and meeting the defined requirements. The evaluation was carried out in two stages: first without, and then with the support of GDPR-Pilot.

3. Problem explication

This section presents the theoretical foundations of the GDPR features (Section 3.1), which support the conceptualization and development of our solution artifact, along with a detailed analysis of the survey (Section 3.2) conducted to derive the research questions that guide this work.

3.1. Background on GDPR

The GDPR is applicable to all enterprises operating within the European Economic Area (EEA) as well as those outside the EEA that process the personal data of individuals within the EU, regardless of the location of the enterprise or the citizenship of the Data Subjects involved. In the Eurozone, GDPR compliance is mandatory whenever a business process involves personal data. The regulation has reshaped privacy and data protection requirements, with substantial implications for process design [3]. The GDPR requires *privacy-by-design*, which means that data protection is not an addition to the business process, but rather an integral part of it, and the process should comply with GDPR from the design stage. Therefore, a process designer needs to consider privacy and data protection issues already at this stage. With the increase of systems able to collect data automatically, privacy has been at the center of many discussions between designers who want to use such data to provide services to users, while at the same time sharing minimal information while accessing those services [2].

Entities. To identify who is responsible for handling data within a process, the GDPR defines 4 entities:

- *Data Subject* (Art. 4(1)): an individual about whom data is collected or processed (e.g., a customer of a telecom company, a patient in a hospital, a job applicant, etc.).
- *Data Controller* (Art. 4(7)): person or organization that collects and stores personal data from the Data Subject and determines the purposes and means of processing such data (e.g., a company deciding to collect customer data for marketing, a hospital deciding how and why patient records are stored, etc.).
- *Data Processor* (Art. 4(8)): entity that processes personal data from the Data Subject on behalf of the Data Controller (e.g., a cloud service provider storing customer data for a company, an email marketing service, a payroll processor, etc.).
- *Data Protection Officer (DPO)* (Art. 37): appointed individual responsible for overseeing GDPR compliance within an organization, monitoring the activities of both the Data Controller and Data Processor to ensure that the processing of personal data collected from the Data Subject adheres to GDPR requirements (e.g., a privacy officer in a company or public authority).

Personal data. In the context of the GDPR, *personal data* (Art. 4(1)) is defined as any information relating to an identified or identifiable natural person (Data Subject). An identifiable person is one who can be identified, directly or indirectly, by reference to an identifier such as a name, an identification number, location data, online identifiers including IP address and cookies, etc. The GDPR distinguishes three types of personal data,[4] each with a different level of protection:

- *personal data*: any information that can identify a person.
- *sensible data*: is a special type of personal data that requires a higher level of security, i.e., health, genetic, physical, physiological, mental, economic, cultural, social identity, and biometric data.
- *criminal records*: is a subset of *Sensible Data* including information to identify past crimes committed by the Data Subject.

Obligations of the Data Controller. This paper focuses on designing modeling patterns in BPMN to explicitly specify the obligations of the Data Controller. These obligations primarily concern the operationalization of Data Subject rights and the execution of mandatory communication activities (e.g., breach notifications). They translate into a set of constraints that the Data Controller must fulfill to ensure GDPR compliance throughout business process execution. In particular, they address the following aspects:

- *Notification of Data Breaches*: in case of a data breach, regardless of its magnitude, the Data Controller has to communicate it within 72 h to the Supervisory National Authority as well as to the Data Subject along with the actions that will be performed to limit the damage. The only exception is the case in which the stolen data is not usable, e.g., encrypted (Arts. 33–34).
- *Consent to Use the Data*: when processing personal data, the Data Controller must ensure that it is handled only after obtaining explicit and informed consent from the Data Subject (Arts. 6–7).
- *Right to Access and Rectify*: the Data Controller must provide mechanisms for the Data Subject to access their personal data and rectify any inaccuracies (Arts. 15–16).
- *Right to Data Portability*: the Data Controller must allow the Data Subject to transfer their personal data to another Data Controller in a machine-readable format, if requested (Art. 20).

[4] The only exception is National Security Data that does not follow the GDPR, but is left to the jurisdiction of each State.

- *Right to Object*: the Data Controller must enable the Data Subject to object to certain types of processing, such as direct marketing. Upon such objection, the Data Controller must no longer process the personal data unless they can demonstrate legitimate grounds that override the rights of the Data Subject (Art. 21).
- *Right to Object to Automated Processing*: the Data Controller must respect the Data Subject's objection to decisions based only on automated processing that may significantly affect their rights, such as profiling. Appropriate measures should be implemented by the Data Controller to protect the Data Subject, including suspending or stopping the automated processing or guaranteeing human intervention to review the outcomes of the automated decisions (Art. 22).
- *Right to Restrict Processing*: the Data Controller must enable the Data Subject to restrict the processing of their personal data under specific conditions, such as when the accuracy of the data is contested or the processing is unlawful (Art. 18).
- *Right to be Forgotten*: the Data Controller must guarantee to the Data Subject that their personal data can be deleted upon request, provided no overriding legal grounds for retention exist (Art. 17).

3.2. Survey on handling GDPR constraints in business processes

To motivate the need for explicitly specifying GDPR privacy constraints in BPMN models, we designed and administered a survey of 9 questions to 33 GDPR experts working in different companies and institutions, encompassing diverse professional roles such as researchers, compliance officers, consultants, process analysts, and data scientists, and representing both academic and industry backgrounds. The survey aimed to assess whether prior knowledge of GDPR constraints and their explicit representation in a process model at design-time can improve the management and resolution of privacy issues during process execution (run-time), thereby justifying the focus of this paper. The survey results were analyzed to formulate two research questions that subsequently guided the research presented in this paper.

The survey used a Likert scale, ranging from 1 to 4, to evaluate responses to Q1, Q2, Q6, Q7, Q8, and Q9, as shown in Table 1. On the other hand, Q3, Q4, and Q5 (cf. Tables 2–4) provided pre-defined answer options related to privacy violations, with Q3 and Q4 allowing respondents to select multiple answers, while Q5 permitted only a single response. The complete list of questions is reported below:

- **Q1**: How important do you think it is to comply with the privacy restrictions imposed by the GDPR when executing a business process?
- **Q2**: How often do you witness privacy breaches during a business process execution?
- **Q3**: Which privacy breaches are most likely to be observed when executing a business process?
- **Q4**: In your experience, which are the most complex rights of the Data Subjects (according to the GDPR) to be guaranteed when executing a business process?
- **Q5**: What is the strategy adopted by your company to address GDPR violations?
- **Q6**: Do you think that managing GDPR obligations during the design phase of the process (design-time) rather than during its execution (run-time) can reduce potential negative impacts on the process itself?
- **Q7**: Do you think the availability of well-defined procedures (to be integrated into the process model) for identifying and handling GDPR violations assists the company in resolving them?
- **Q8**: Individual users may contact a company to exercise their rights under the GDPR (rights of access, rectification, erasure, restriction, objection, etc.). Do you think the availability of well-defined procedures for managing GDPR obligations may positively affect user satisfaction (e.g., response time, etc.)?

Table 1
Answers related to Q1, Q2, Q6, Q7, Q8 and Q9.

Likert scale	1: Not at all	2: Slightly	3: Moderately	4: Very
Q1	0%	0%	18,2%	81,8%
Q6	0%	9,1%	24,2%	66,7%
Q7	3%	6,1%	24,2%	66,7%
Q8	0%	9,1%	27,2%	63,6%
Q9	0%	9,1%	36,4%	54,5%
Likert scale	**1: Never**	**2: Rarely**	**3: Occasionally**	**4: Often**
Q2	12,1%	24,2%	54,5%	9,1%

- **Q9**: Do you think that the availability of a well-defined methodology that identifies GDPR constraints at design-time and integrates their management within business processes can make their handling more efficient during process execution?

Questions Q1, Q2, Q3, Q4, Q5 and Q6 aim to assess GDPR experts' awareness of privacy issues at the design stage and their perception of the importance of GDPR compliance during process execution. From the response analysis, the following observations emerged:

- Responses to Q1 indicate that the majority of the experts (27 out of 33) consider compliance with GDPR privacy restrictions during process execution to be very important. Notably, none of the respondents rated this compliance as unimportant or only slightly important.
- Responses to Q2 show that nearly two-thirds of the surveyed experts (21 out of 33) have directly observed multiple privacy breaches during process execution, whereas only 4 reported never encountering such cases. Interestingly, Q3 reveals that most of the breaches experienced (or anticipated) were associated with unauthorized access or disclosure of personal data, as well as loss of data availability.
- Responses to Q4 reinforce the findings from Q3. In particular, the rights to data portability and to be forgotten emerged as the most complex to operationalize within business processes. These rights are highly sensitive to privacy breaches, particularly unauthorized access or disclosure of personal data, which complicates their enforcement at the business process level.
- Responses to Q5 indicate that the vast majority of institutions and companies where the surveyed experts are employed (28 out of 33) implement ad-hoc internal procedures to manage GDPR violations. Moreover, responses to Q6 clearly highlight that incorporating policies to handle GDPR obligations at design-time could significantly reduce negative impacts during process execution.

To summarize, the results from Q1–Q6 highlight not only the importance of managing GDPR obligations during process execution, but also the value of integrating privacy constraints into process models at design-time. These findings strengthen our objective of providing a general-purpose solution that captures GDPR privacy constraints as design patterns and integrates them into standard BPMN models, motivating the formulation of a first research question:

RQ1: *How can process models be developed to handle GDPR constraints, and what are the various types of constraints that can be encountered?*

Subsequently, questions Q7, Q8 and Q9 examine the surveyed experts' perceptions of the usefulness, for both companies/institutions and Data Subjects exercising their data privacy rights, of embedding clear procedures directly into process models to predefine the management of GDPR violations at design-time. The results reveal a near-unanimous agreement that the availability of an approach making process models GDPR-aware at design-time would be more effective than addressing GDPR violations at run-time during process execution. Based on these findings, we derived a second research question to explore the effectiveness of adopting such an approach:

Table 2
Answers related to Q3.

Q3: Which privacy breaches are most likely to be observed when executing a business process?	
Access by an unauthorized third party	69,7%
Unauthorized disclosure of personal data	66,7%
Loss of availability of personal data due to accidental or/and deliberate causes	45,5%
Destruction or damage of personal data	36,3%
Computing devices containing personal data being lost or stolen	30,3%

Table 3
Answers related to Q4.

Q4: In your experience, which are the most complex rights of the Data Subjects (according to the GDPR) to be guaranteed when executing a business process?	
Right to Data Portability, Right to be Forgotten	42,4%
Right to Restrict Processing, They are all complex to manage	24,2%
Right to Object, Rights to Object to Automated Processing	21,2%
Right to Rectify, Right of Access, Right to be Informed	9%
They are all simple to manage	6%

Table 4
Answers related to Q5.

Q5: What is the strategy adopted by your company to address GDPR violations?	
Internal procedures enacted by the company	84,8%
Third-party support	9,1%
I don't know	6,1%

RQ2: *To what extent is an approach that integrates various privacy-constraint patterns into a business process model effective?*

In Section 6, we address RQ1 by introducing a methodology that demonstrates how the GDPR privacy constraints can be captured in BPMN models, thereby enabling GDPR awareness at design-time. RQ2 is addressed in Section 7, where the methodology is first demonstrated to establish its feasibility and subsequently evaluated against the requirements presented in Section 5.

4. Related work

The BPM literature offers a wide range of approaches for extending process models with additional elements that capture external requirements needed to represent complex real-world scenarios [23,24]. In particular, numerous BPMN extensions have been proposed to integrate security and privacy requirements at design time by augmenting existing process models with dedicated modeling constructs. In this context, to guide the systematic extension of BPMN and address a broad spectrum of cybersecurity concepts, the authors of [25,26], and [27] have proposed dedicated ontologies that define the key concepts for the development of BPMN security extensions. Nonetheless, most literature works have realized their own BPMN extensions independently.

For example, in the healthcare domain, the works [28] and [29] extend BPMN with new security constructs that can be integrated into process models for developing security-aware healthcare procedures, while in [30] the authors propose integrating custom privacy constraints into BPMN by leveraging DMN (Decision Model and Notation [31]) to help decision makers in determining if the use of personal data in a clinical procedure is justified.

In [11], the authors introduce new security elements for process modeling that allow the abstract specification of objectives like confidentiality and integrity directly within BPMN models. In [12], the authors introduce SecureBPMN, a BPMN extension aimed at aligning business processes with the IAS (Information Assurance & Security) domain [32] and identify process fragments potentially vulnerable to security threats. Similarly, in [14], the authors propose a BPMN extension for security risk management based on the BPMN alignment to the ISSRM (Information System Security Risk Management) concepts [33]. In [17], the authors introduce SecBPMN-ml, a security-focused extension of BPMN designed to represent custom security policies, which can subsequently be queried using the SecBPMN-Q query language. In [6], the authors introduce PE-BPMN, a privacy-enhanced extension of BPMN to model collections of autonomous systems executing collaborative processes protected by privacy-enhancing technologies. Building on [6], in [7] the authors realize an approach for verifying that the technologies specified in a PE-BPMN model are correctly applied, ensuring that no unintended data disclosures occur during process execution. In [13], the authors extend BPMN choreography diagrams to incorporate identity-related privacy requirements, aiming to present these aspects in a process-oriented view that is understandable by IT professionals involved in inter-organizational information systems initiatives. In [15], the authors introduce a novel security modeling language integrated into BPMN to capture security requirements. Similarly, in [16], BPMN is extended with new constructs for modeling privacy requirements, expressed using the Semantic Web Rule Language (SWRL), which enables the application of reasoning tools to verify and enforce privacy constraints at run-time. More recently, in [20], an approach is proposed for annotating BPMN entities with high-level, non-security-related information. These annotations are then used to automatically identify potential threats using the ENISA Threat Landscape[5] and to assess risks based on the OWASP Risk Rating Methodology.[6]

Unlike the aforementioned studies, which address the integration of various cybersecurity and privacy constraints into business processes at design-time or run-time, our work focuses specifically on representing GDPR privacy requirements as design patterns that can be directly integrated into BPMN-based models, presenting a proactive approach to capture privacy constraints prior to process execution. Since the introduction of the GDPR in 2018, numerous studies in the BPM field have proposed approaches for developing GDPR-compliant processes.

In [34], the authors propose a method to support the design of GDPR-compliant systems, based on a socio-technical approach composed of a novel modeling language and a reasoning framework. In [35], the authors propose a visual model of the GDPR that illustrates the relationships between legal entities and their associated constraints. In [36], an integrated framework is introduced for representing legal knowledge using established ontologies for GDPR, such as the

[5] https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024
[6] https://owasp.org/www-community/OWASP_Risk_Rating_Methodology

LKIF[7] and PrOnto [37], and rule-based languages like LegalRuleML.[8] This framework is used in conjunction with BPMN and the Regorous engine [38] to detect and prevent privacy rule violations. Building on these works, in [18] the authors propose enriching BPMN with new annotations and connectors to represent GDPR data protection requirements within processes. At run-time, a recommender system is used to provide auditors and supervisory authorities with a process view and the data protection measures in place.

Among the most recent contributions addressing the challenge of integrating GDPR controls into business processes, the works by [39, 40] address GDPR compliance in Big Data systems by proposing a framework to analyze GDPR requirements and translate them to IT design requirements, potentially useful for realizing future GDPR-aware BPMSs. Similarly, in [41] the authors present a tool-supported method for privacy analysis of process models, which aids in eliciting system requirements necessary for GDPR compliance.

The authors of [19] explore how organizations can manage consent and revocation under the GDPR through their business processes. They propose extending BPMN with custom labels to specify consent and revocation controls within workflows, ensuring GDPR compliance at design-time. In [10], the authors present a reference data model that formalizes key GDPR concepts, along with a methodology that enables process designers to evaluate the compliance of existing BPMN models against this data model. In [42], the authors present a blockchain-based tool that supports GDPR compliance checking and trust in business processes at run-time, enabling obligation verification without relying on a trusted third party. Finally, in [8], the authors propose a GDPR compliance framework focused on Articles 33 and 34, which addresses personal data breach notification and communication. The framework includes the definition of data and business process models, along with post-design evaluation and simulation of compliance scenarios.

Compared to the approaches discussed above, the main advantage of our methodology lies in the use of design patterns that integrate GDPR principles without requiring any extensions to the BPMN notation. This is a significant strength, as it enables compliance checks directly at design-time and supports automation in any BPMS that accepts standard BPMN models. In contrast, existing approaches introduce custom BPMN extensions, requiring designers to learn new constructs and necessitating modifications to BPMSs to interpret the extended notation.

5. Requirements and use case definition

In this section, we begin by outlining the requirements that guided the design of our solution (Section 5.1). Next, we introduce the key concepts needed to model a BPMN process, including a concise overview of BPMN, essential for understanding how GDPR-related design patterns can be incorporated into an existing process model (Section 5.2). Finally, we present a motivating use case based on a SIM activation process carried out by a phone company, which serves as the running example throughout the paper (Section 5.3).

5.1. Design requirements

According to [21], a design science research artifact should satisfy a certain number of *structural*, *usage* and *generic environmental* requirements. Structural requirements are concerned with the structure of the artifact. Usage requirements describe how the artifact works and how it is perceived in practical use. Generic environmental requirements describe how the artifact is structurally related to its environment.

With respect to structural requirements, our analysis concentrates on the *modularity* of the artifact. Modularity denotes the extent to which the artifact can be decomposed into distinct components that may be independently separated, reused, and recombined as required. In our context, in which the artifact consists of GDPR design patterns modeled in BPMN, modularity means structuring GDPR patterns as reusable building blocks that can be flexibly integrated into different business processes while maintaining separation from domain-specific logic.

For usage requirements we rely on three aspects, namely the *comprehensibility* (the ease with which an artifact can be understood by a user), *customizability* (the degree to which an artifact can be adapted to the specific needs of local practice), and *learnability* (the ease with which a user can learn to use an artifact) [21]. In our setting:

- Comprehensibility requires that GDPR patterns are expressed in a way that makes their purpose and compliance function immediately clear to Data Controllers.
- Customizability reflects the need for patterns to be adaptable to the specific organizational and contextual variations of GDPR obligations, while preserving their underlying compliance structure.
- Learnability requires that GDPR patterns are designed so that new users can readily understand how to apply and reuse them correctly.

For the generic environmental requirements, we focus on *correctness*. In the context of design science research, correctness refers to the extent to which an artifact functions as expected and produces valid outcomes in its intended environment [21]. With respect to our methodology, correctness implies that BPMN models augmented with GDPR patterns accurately comply with the applicable GDPR regulatory interpretations. Section 7 examines the extent to which our proposed methodology fulfills the requirements identified above.

5.2. Business process modeling and notation (BPMN)

BPMN is a standard graphical language developed by the Object Management Group (OMG) to design process models with an emphasis on the control flow. BPMN defines a flowchart including a range of constructs: (*i*) *flow objects*, (*ii*) *data*, (*iii*) *connecting objects*, and (*iv*) *pools*. Our methodology relies on a standard subset of BPMN elements covering both data and control flow components, including those in the phone company process model in Fig. 2, which depicts the process of activating and delivering a new SIM card to a customer upon request.

Flow objects. *Flow objects* define the behavior of a process and can be classified into *events*, *activities*, and *gateways*. *Events* model anything that can happen instantaneously in the process. They are partitioned into three types. *Start events*, depicted with thin-bordered circles with no incoming sequence flow edges (e.g., the initial event in the phone company process indicating that a new SIM request has been received), are used to trigger processes and create tokens.[9] *Intermediate events*, represented as double-bordered circles with both an incoming and an outgoing sequence flow edge, can delay processes or be triggered during process executions (e.g., the catch message event for receiving customer's personal data). Some intermediate events can be used to throw exceptions during the execution of an activity, such as the error event "Invalid customer data detected" (depicted with a lightning bolt), which is attached to the boundary of the activity "Check correctness of personal data". *End events*, modeled as thick-bordered circles with no outgoing sequence flow edges, mark process completion and token destruction (e.g., the finalization of the procedure). A specific variant, the *terminate end event*, depicted as an end event with a black inner circle, triggers the immediate process termination (e.g., "Procedure aborted") and destroys all tokens within the process instance.

[7] https://github.com/RinkeHoekstra/lkif-core
[8] https://www.oasis-open.org/committees/legalruleml/

[9] Tokens are a conceptual tool to describe the execution flow of a process instance as it progresses through the flow objects of the model.

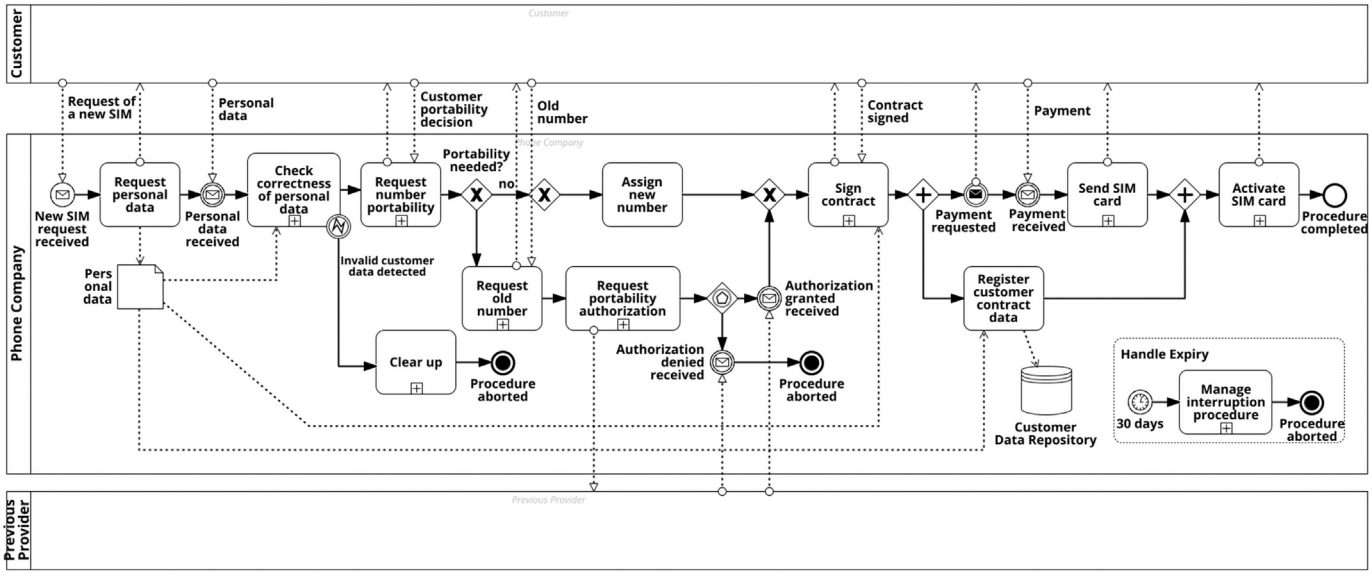


Fig. 2. BPMN model for the case of the phone company.

Activities, depicted as labeled rounded boxes, represent units of work that, unlike events, have a duration. Simple activities (e.g., "Assign new number") are called *tasks*, while those that can be decomposed into smaller work units are called *sub-processes* (e.g., "Sign contract" can be decomposed into "Prepare contract draft", "Review contract", etc.). *Event sub-processes*, delimited by a dotted rounded rectangle, are triggered by dedicated start events (such as timers, messages, errors, signals, etc.). These subprocesses provide a global mechanism for handling external messages, exceptions, or specific conditions that may arise during the execution of the main process, such as deadline expiration, etc. In the latter scenario, the exception is caught by the event subprocess responsible for recovery, which handles the expiry of the procedure if the process instance remains incomplete after 30 days.

Gateways control the splitting and joining of process flows to represent conditions like mutual exclusion or concurrency. *Split gateways* have one incoming and multiple outgoing edges, branching the flow, while *join gateways* merge flows with multiple incoming and one outgoing edge. The main gateway types are *exclusive* (XOR), *parallel* (AND), and *event-based*. *XOR gateways* model mutually exclusive paths, where only one is executed according to a data-driven condition (e.g., the gateway that checks whether the customer has requested number portability). *AND gateways* model the relation between two or more paths that can be executed concurrently: they have no order dependencies but must all be executed (e.g., the gateway preceding the activities for registering the customer's contract data and the event for requesting payment). Specifically, the AND-split enables parallel branches, and the AND-join merges them once all are complete. *Event-based gateways* model races between multiple events, whichever occurs first determines how the process proceeds. They have one incoming and multiple outgoing edges, each linked to a possible event. When reached, process execution pauses until one of the events occurs. It is used in Fig. 2 to model the phone company waiting for authorization (granted or denied) regarding number portability from the previous provider.

Data. BPMN allows the explicit modeling of data (e.g., applications, contracts, etc.) using *data objects* and *data stores*. *Data objects* specify data inputs and outputs of activities. *Data stores* are places containing data objects that need to persist beyond the duration of a process instance, e.g., a database.

Connecting objects. The *sequence flow* is used to specify the ordering of flow objects, while *message flow* describes the flow of messages between business partners represented by pools. *Association* is a specific type of connecting object that is used to link data objects/stores to activities.

Pools and Lanes. From a resource perspective, *pools* model resource classes, i.e., independent organizational entities that do not share any common system, but communicate with each other through messages (e.g., the customer, the company and the previous provider). *Lanes* represent organizational entities (e.g., departments, teams, or resources) within a pool, visually dividing the process flow to show responsibility for each part.

5.3. Use case

We now introduce a real-world use case concerning the handling of personal data and the corresponding management of GDPR constraints.[10] As a running example, we consider a phone company managing the activation and delivery of a new SIM card to a customer upon request. The BPMN model representing this scenario is shown in Fig. 2 and involves collecting, exchanging and storing personal data, thus triggering multiple GDPR obligations for the Data Controller.

The phone company initiates the process by requesting the customer's personal data (e.g., name, surname, address). Once the data is collected, a verification subprocess is executed to ensure its correctness. In case the data is found to be inaccurate, an exception flow is triggered, activating a cleanup sub-process that leads to the termination of the process. Otherwise, the prospective customer is asked whether they wish to port their existing phone number into the new subscription plan. If the customer opts for number portability, the phone company requests the old phone number and initiates the portability procedure by interacting with the previous provider. If the previous provider denies authorization for the portability of the old number (e.g., due to contractual constraints), the process instance is aborted. Otherwise, the customer signs the contract outlining the provision of the service by the phone company; however, the contract does not specify how the company will process and use the customer's personal data. Subsequently,

[10] In the appendix, we describe two additional use cases, related to a hiring process and a healthcare procedure, both used in the evaluation of the methodology in Section 7.2

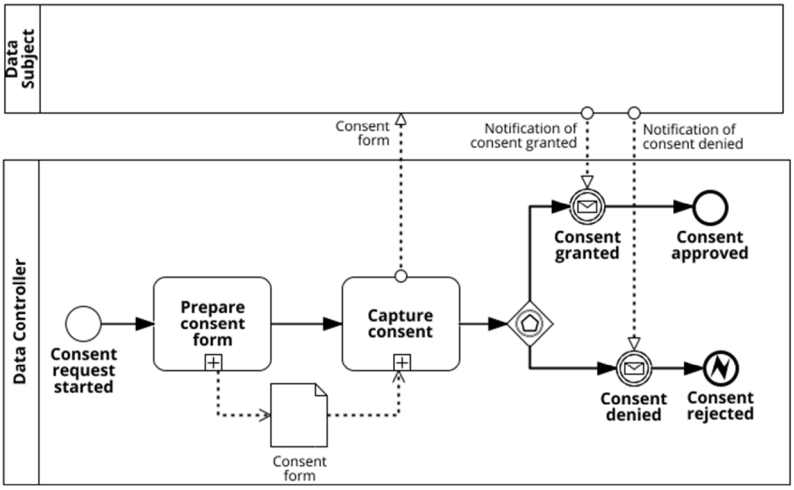


Fig. 3. BPMN model for pattern *Consent to Use the Data*.

the phone company stores the new customer's personal data and requests payment. Once the payment is received, the SIM card is shipped to the customer. After delivery, the company activates the SIM card, thereby successfully concluding the procedure. However, if the process takes longer than 30 days to complete, the process is interrupted.

It is worth noting that, at this stage, the procedure does not account for potential data breach risks and lacks mechanisms to protect the customer's privacy or to enforce the rights guaranteed under the GDPR. We will discuss in the next section how this process can be transformed into a GDPR-aware one using our methodology.

6. Design and development

Under Art. 25 of the GDPR, Data Controllers must implement appropriate technical and organizational measures that embed data protection principles at design-time and during data processing. If a privacy issue arises at run-time, countermeasures only resolve the single affected execution, meaning the problem can recur. By contrast, a design-time modification applies to all future executions, ensuring long-term compliance. At design-time, business processes are described through process models, which capture activities and conditions independently of execution. To ensure GDPR compliance at design-time, process models must incorporate the Data Controller's obligations.

To address RQ1, this section first presents how we modeled the GDPR privacy constraints introduced in Section 3.1 as BPMN design patterns, explaining the rationale behind our choices (Section 6.1). Then, we introduce a methodology for integrating these patterns into existing process models, clarifying when and how each should be applied (Section 6.2). Finally, we present the software architecture of GDPR-Pilot, a BPMN editor developed to support a Data Controller in applying our methodology (Section 6.3).

6.1. Pattern development

We introduce nine privacy patterns for BPMN, designed as effective design-time solutions to address GDPR constraints in process models. These patterns require no additional BPMN symbols, either to represent their behavior or to integrate them into existing, non-GDPR-compliant models. Each pattern has been derived from the procedural steps outlined in the GDPR obligations. For each, we: (i) provide a brief introduction to the corresponding GDPR requirement; (ii) specify the BPMN model by detailing the steps needed to fulfill the obligation.

Consent to Use the Data. As outlined in the Arts. 6–7 of the GDPR, before collecting any personal data from the Data Subject, the Data Controller must obtain their consent. The design pattern in Fig. 3 implements the privacy constraint *Consent to Use the Data*, modeled in BPMN.

By examining the BPMN model in Fig. 3, we can see that the first activity performed by the Data Controller is "Prepare consent form" that must communicate: (i) the purpose of the data processing; (ii) which personal data will be processed; (iii) the legal basis for collecting and processing such data, referencing GDPR Arts. 6–7; (iv) the rights of the Data Subject, including access, rectification, and withdrawal of consent; (v) which data are mandatory and which are optional; and (vi) the procedures and contacts for revoking consent. Once the form is prepared, it is sent to the Data Subject via the "Capture Consent" activity, which ensures that the Data Subject provides explicit and informed consent before any personal data is processed. If consent is granted, the personal data are collected within the scope of the process implementing this pattern. Conversely, if consent is denied, the procedure terminates by triggering an exception through an end error event, which determines the abortion of the process (see also Fig. 13).

Right to Access. As reported in the Art. 15 of the GDPR, the Data Controller is required to establish mechanisms that enable the Data Subject to access their personal data upon request. The design pattern in Fig. 4 implements in BPMN this obligation for the Data Controller.

The pattern is initiated when a Data Subject submits a request via email, form, or another channel. In response, the Data Controller collects all personal data and associated processing/elaboration records from the internal databases, excluding any information subject to restrictions (e.g., data that also pertains to third parties). The Data Controller then prepares a data access report specifying whether personal data is being processed, for what purposes, the applicable storage or retention periods (or the criteria used to determine them), and the source of the data (if it was not collected directly from the Data Subject). The report is sent to the Data Subject, with explanations for any data that cannot be provided (e.g., to protect others' rights).

Right to Data Portability. According to Art. 20 of the GDPR, the *Right to Data Portability* requires the Data Controller, upon the Data Subject's request, to transmit the Data Subject's personal data to another Data Controller in a machine-readable format. The design pattern illustrated in Fig. 5 models in BPMN this GDPR constraint.

When the Data Subject submits a request to exercise the right to transfer their data to a third-party Data Controller, they must indicate the original Data Controller to whom the data should be requested. The third-party Data Controller then contacts the original Data Controller holding the personal data. In response, the original Data Controller

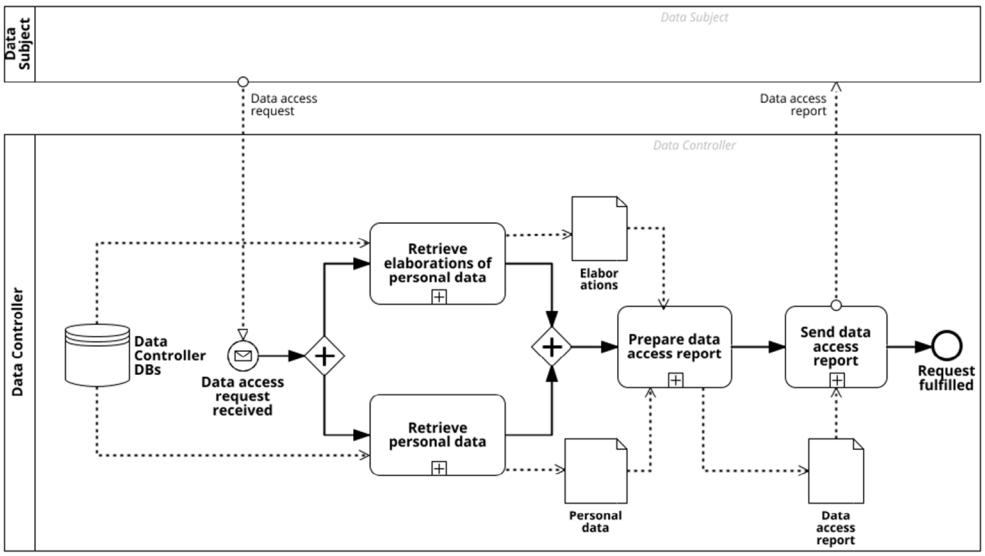


Fig. 4. BPMN model for pattern *Right to Access*.

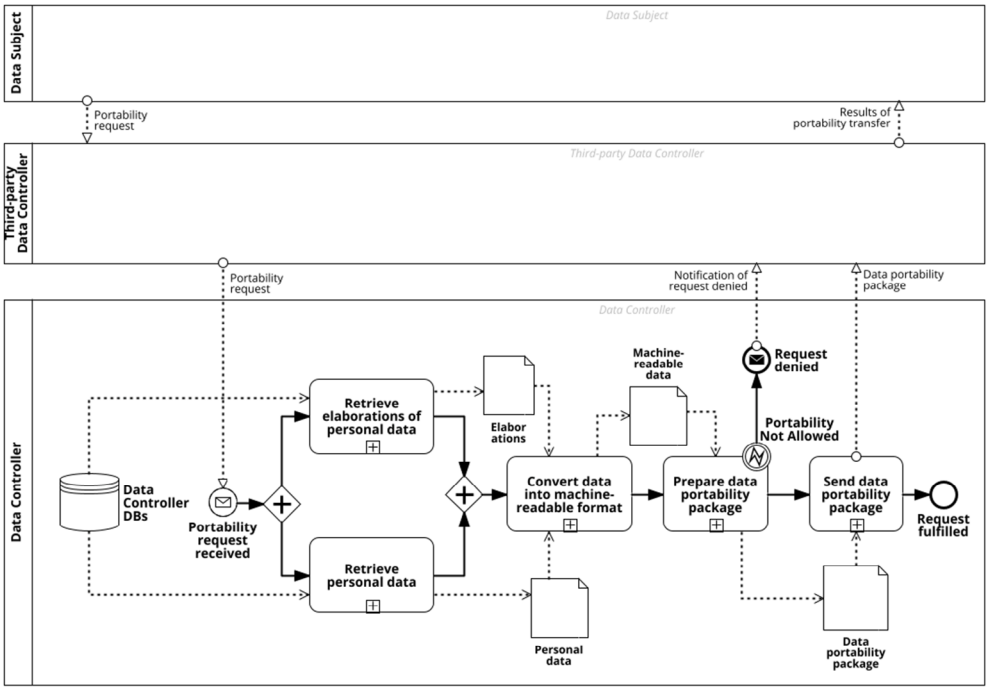


Fig. 5. BPMN model for pattern *Right to Data Portability*.

retrieves all personal data provided by the Data Subject and the elaborations of data generated through their processing activities. Then, the original Data Controller converts the data into a machine-readable format (e.g., CSV, XML, JSON), thus ensuring interoperability with other systems. If the portability request is deemed technically and legally feasible (otherwise, a denial notification is sent to the third-party Data Controller and communicated to the Data Subject), the original Data Controller prepares a data portability package that includes: (i) the requested personal data; (ii) the transfer format; and (iii) any limitations arising from legal or technical constraints. This package is then transmitted to the third-party Data Controller, who in turn notifies the Data Subject of the successful transfer.

Right to Rectify. Under Art. 16 of the GDPR, the *Right to Rectify* requires the Data Controller to correct or complete any inaccurate or incomplete personal data upon the Data Subject's request. The design pattern depicted in Fig. 6 models in BPMN this GDPR obligation for the Data Controller.

When a Data Subject submits a request to exercise their right to rectification, the Data Controller identifies all instances of the personal data that require correction and updates them. In some cases, the request may not be fulfilled (e.g., due to legal or regulatory constraints). Regardless of the outcome, the Data Controller must inform the Data Subject that the rectification request has been processed, providing a clear explanation if the rectification was denied. Moreover, the Data Controller must notify all recipients (i.e., third-party organizations) who have received the personal data of the rectification, enabling them to update their records accordingly. This ensures that every copy of

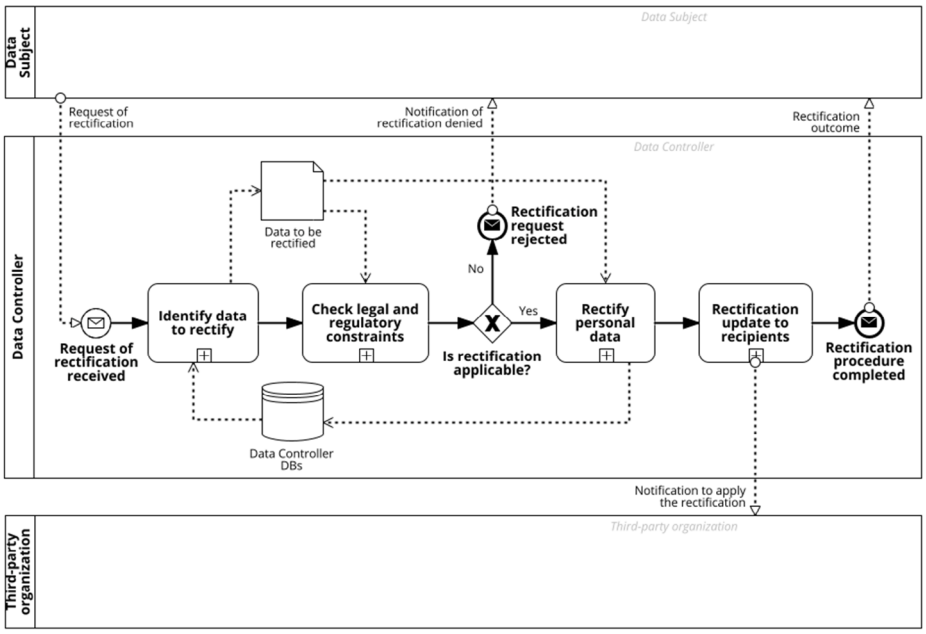


Fig. 6. BPMN model for pattern *Right to Rectify*.

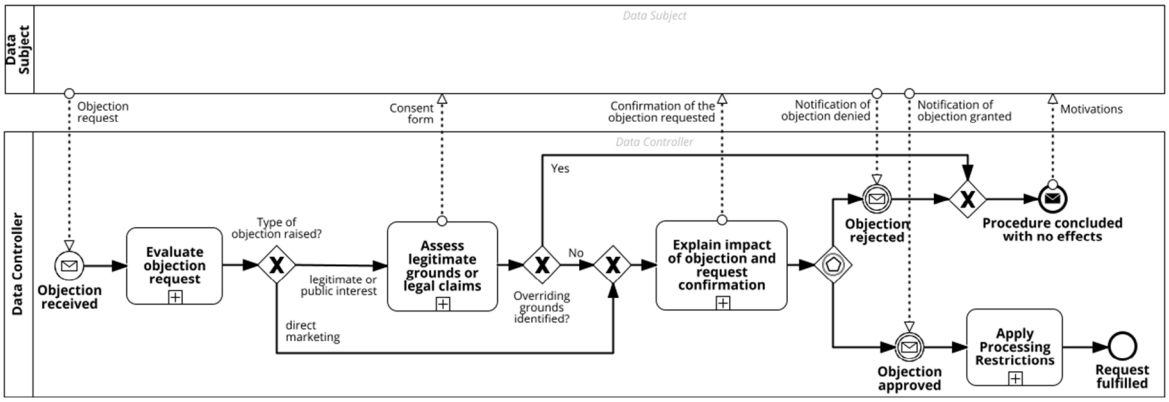


Fig. 7. BPMN model for pattern *Right to Object*.

the personal data remains accurate and consistent, in compliance with GDPR requirements.

Right to Object. The *Right to Object* (Art. 21 of the GDPR) allows the Data Subject to oppose the processing of their personal data at any time, particularly when processing is based on legitimate or public interests, or for direct marketing purposes. The pattern in Fig. 7 models in BPMN this GDPR constraint for the Data Controller.

The pattern begins when the Data Subject submits a request of objection specifying the type of processing they oppose. The Data Controller evaluates the request. If the objection concerns direct marketing, the processing must stop. Conversely, if the objection relates to legitimate or public interest, the Data Controller assesses whether legitimate grounds exist to continue processing. If no overriding grounds are identified, data processing must stop, and the data may need to be deleted or restricted. Before enacting any restriction or deletion, the Data Subject is informed that upholding the objection will result in the termination of all running processes that rely on those data. If the Data Subject confirms their intention to proceed, the processing restrictions are applied and all such processes must be stopped. Otherwise, if the Data Subject withdraws the objection or if overriding grounds exist, the processing of personal data continues, with the decision clearly justified and communicated to the Data Subject.

Right to Object to Automated Processing. The *Right to Object to Automated Processing* (Art. 22 of the GDPR) grants Data Subjects the right not to be subject to decisions based solely on automated processing, including profiling, that may produce legal effects affecting them. Data Subjects can even request human intervention to contest and review the decision. The pattern in Fig. 8 specifies in BPMN this GDPR obligation.

The pattern begins when the Data Subject submits a request objecting to automated decision-making, specifying the processing activity being contested. The Data Controller identifies the automated system and the personal data involved, and evaluates whether the request is applicable. If it is not applicable (e.g., the data processing is not solely automated or does not produce significant effects), the Data Controller informs the Data Subject and terminates the procedure. On the other hand, if the request is applicable, the Data Controller checks whether the automated processing is legally justified by contractual necessity, law, or explicit consent. If no such justification exists, processing must stop. If justification is present, processing may continue but with safeguards in place, such as human intervention and an appeal mechanism. Where human review is delegated, the reviewer reassesses the decision in light of the Data Subject's input. If the decision is overturned by the human reviewer, the automated decision is updated or withdrawn. Finally, the Data Subject is notified through a report that explains whether processing will continue or stop, summarizing the reviewer's

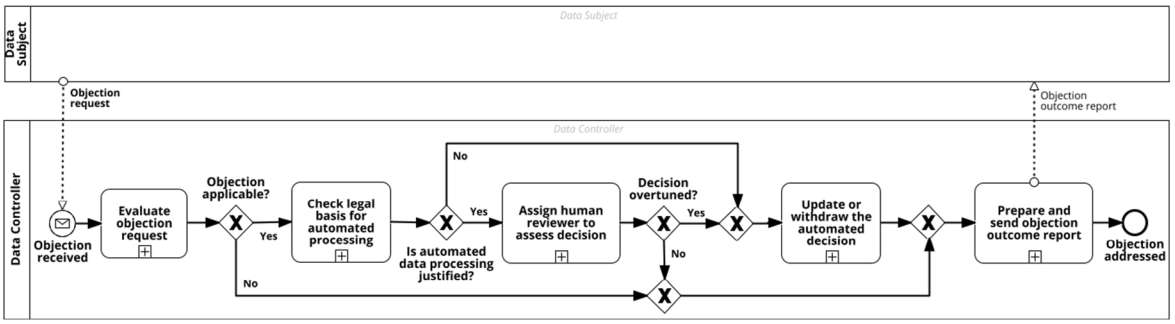


Fig. 8. BPMN model for pattern *Right to Object to Automated Processing*.

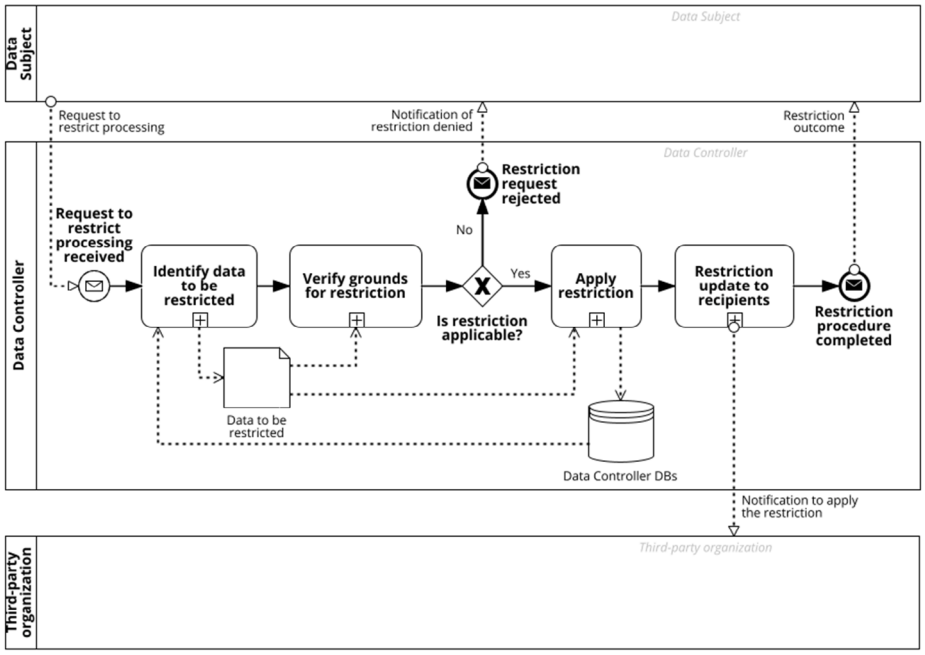


Fig. 9. BPMN model for pattern *Right to Restrict Processing*.

assessment (if involved), and specifies the justification of the decision together with available remedies (e.g., appeal mechanisms).

Right to Restrict Processing. The *Right to Restrict Processing* (Art. 18 of the GDPR) allows the Data Subject to request that the Data Controller temporarily limits the use of their personal data. During the period of restricted processing, data may only be stored or processed for limited purposes (e.g., with the data subject's consent, for legal claims, or for important public interest). The pattern in Fig. 9 models in BPMN this GDPR constraint for the Data Controller.

When a Data Subject submits a restriction request, the Data Controller first identifies the personal data affected and then assesses the request's validity by checking whether grounds for restriction are met (e.g., processing is unlawful but deletion is opposed, data is no longer needed but required for legal obligations, or a pending objection to processing exists). If the request is deemed inapplicable, the Data Controller notifies the Data Subject of the rejection, and the procedure ends. If the request is legitimate, the Data Controller applies the restriction by marking the personal data as "restricted" in the internal databases, blocking further processing except for storage, consent-based processing, legal claims, or public interest purposes. Finally, the Data Controller notifies all recipients (i.e., third-party organizations) who have received the personal data to enforce the restriction, and then informs the Data Subject that the restriction has been applied.

Right to Be Forgotten. According to Art. 17 of the GDPR, the *Right to Be Forgotten* allows a Data Subject to request the deletion of their personal data when it is no longer necessary for the purpose it was collected. The pattern in Fig. 10 models in BPMN this GDPR constraint for the Data Controller.

When a Data Subject submits a deletion request, the Data Controller first verifies its legitimacy (e.g., data no longer needed, consent withdrawn, processing unlawful). If the request is inapplicable, the Data Controller notifies the Data Subject and terminates the procedure. If legitimate, the Data Controller identifies all instances of the Data Subject's personal data across internal databases and assesses whether legal, contractual, or public interest constraints require retaining some data. If retention is necessary, partial deletion is applied, and the Data Subject is informed of the exceptions. Otherwise, all relevant data are deleted. The Data Controller then instructs any third-party recipients to erase the data and finally confirms to the Data Subject that their data have been deleted.

Notification of Data Breaches. Data breaches are regulated under Arts. 33 and 34 of the GDPR, requiring the Data Controller to notify the supervisory authority and, when the breach poses high risk, inform the affected Data Subjects. The pattern in Fig. 11 specifies with BPMN this GDPR constraint for the Data Controller.

In the event of a data breach, which is typically triggered by a security incident, a system alert, or an employee report, the Data Controller must first assess its nature and scope. This includes: (i) determining what personal data was affected; (ii) identifying the categories of Data

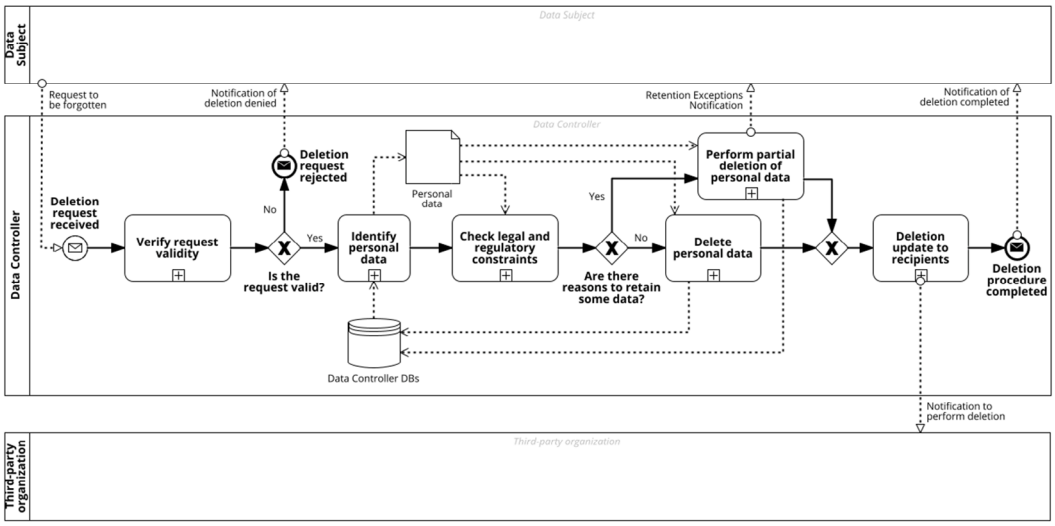


Fig. 10. BPMN model for pattern *Right to be Forgotten*.

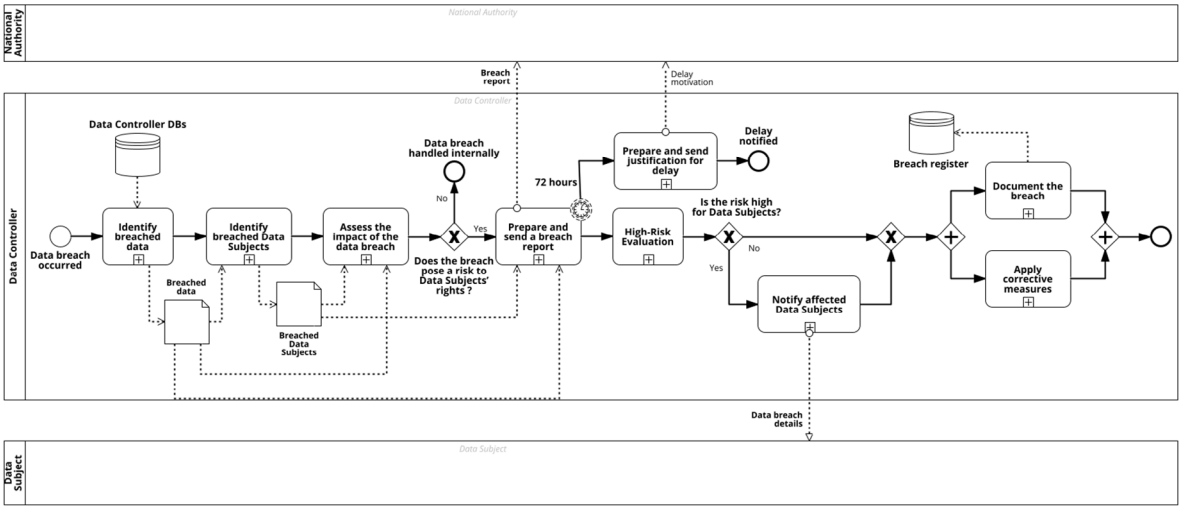


Fig. 11. BPMN model for pattern *Notification of Data Breaches*.

Subjects involved; and (iii) evaluating the potential impact on their rights. If no risk to Data Subjects' rights is identified, the breach is handled internally and the procedure concludes. Otherwise, within 72 h of becoming aware of the relevance of the breach, the Data Controller must notify the National Supervisory Authority by sending a breach report that specifies the type of the breach, the data and Data Subjects affected, contact details of the DPO appointed by the Data Controller, possible consequences and planned mitigation measures. If the Data Controller does not notify the National Authority within 72 h, they must provide a justification for the delay. In the BPMN model, this is represented by a non-interrupting timer boundary event, which allows the preparation and submission of the delay justification without interrupting the ongoing activity of drafting the breach report. In the next stage, the Data Controller evaluates whether the breach poses a high risk to Data Subjects' rights. If not, mitigation measures (e.g., security patches, access revocations, etc.) are applied, and the incident is recorded in the internal breach register with all justifications and notifications. If the risk is high, the Data Controller must also notify the affected Data Subjects, explaining the nature of the breach, potential consequences, mitigation actions, and available rights and remedies.

6.2. Extending a BPMN process model with GDPR patterns

To integrate GDPR patterns into a non-GDPR-compliant process model, the Data Controller must first identify the process fragments where potential GDPR violations could occur and determine which patterns need to be applied. To assist Data Controllers in this task, we developed a straightforward procedure, illustrated in Fig. 12, which provides a series of questions to determine *whether* a specific pattern is required to achieve GDPR compliance.

The first question (A) determines if the process under analysis involves handling personal data. If not, none of the GDPR constraints apply, since GDPR patterns are only relevant when personal data from the Data Subject is collected, stored, or processed. If personal data is involved, the Data Controller must then verify whether consent to process the data has already been obtained (B). If consent has not been obtained, the *Consent to Use the Data* pattern must be implemented in the process. In addition, because personal data is being managed, the *Notification of Data Breaches* pattern must also be applied to define mitigation and communication procedures in case of data compromise. The following questions (from C to I) can then be assessed in any order, each addressing whether the exercise of a specific Data Subject right is relevant in the given process. If so, the corresponding GDPR pattern must be incorporated into the process model.

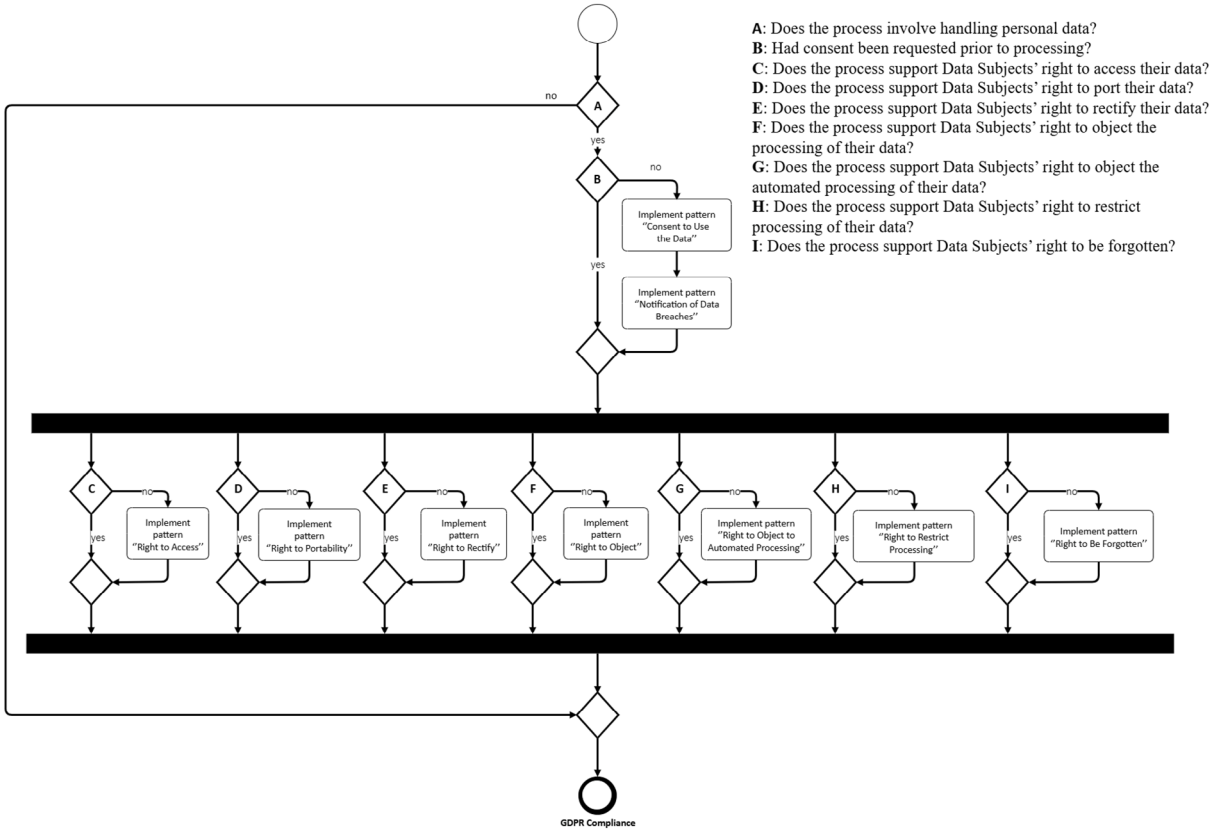


Fig. 12. A methodology to decide when a GDPR pattern should be integrated into a process model.

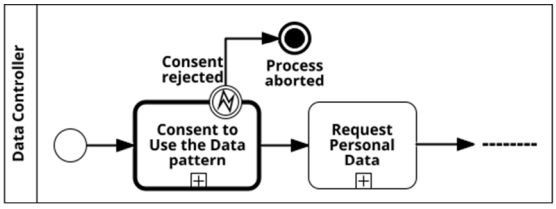
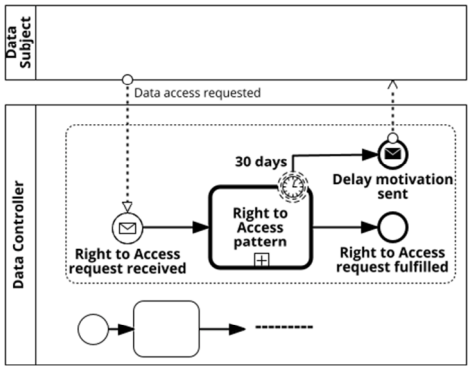


Fig. 13. Positioning of the *Consent to Use the Data* pattern.

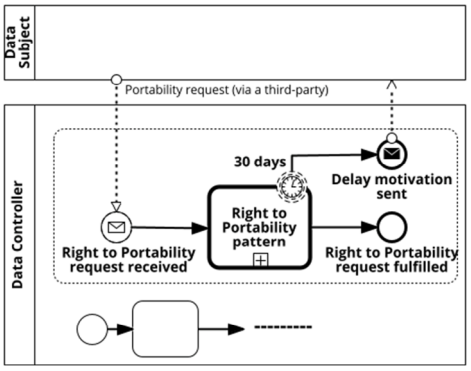
Concerning *where* a specific GDPR pattern should be inserted into an existing process model, the *Consent to Use the Data* pattern must be positioned immediately before the first activity that collects or processes personal data during process execution, as illustrated in Fig. 13. In practice, identifying this activity may not always be straightforward. While a process model might explicitly include an activity named "Request Personal Data", in many cases data collection is expressed using different labels, such as "Ask for Personal Data", "Retrieve Personal Data", "Request Personal Information", or "Request Details". Therefore, the Data Controller must carefully analyze the process model to recognize such activities and ensure consent is obtained beforehand. From a technical perspective, the *Consent to Use the Data* pattern can be implemented as a *Call Activity* in BPMN. A Call Activity is a special kind of subprocess that references and reuses an independently defined procedure. This means the consent-handling pattern can be modeled once as a standalone subprocess (like in Fig. 3) and then invoked wherever personal data processing is initiated in different process models. Note that, if consent is denied, the process will be aborted, as the required services or products cannot be provided without the customer's personal data.

Unlike the *Consent to Use the Data* pattern, which represents a *proactive* obligation, the *Notification of Data Breaches* pattern is a *reactive* constraint triggered by an external event, such as a report from the DPO or the National Authority, when a data breach occurs. Accordingly, this pattern is incorporated into the process as an event subprocess, allowing it to capture external triggers at any point and immediately execute the remedial activities defined in the pattern. These activities are implemented as a Call Activity, as illustrated in Fig. 14(h). Similarly, all patterns related to Data Subject rights are also reactive, as they are triggered by an external request from the Data Subject at any point during process execution. For this reason, also these patterns are integrated into the process using an event subprocess that executes the corresponding pattern logic. As illustrated in Figs. 14(a), 14(b), 14(c), 14(d), 14(e), 14(f), and 14(g), all subprocesses implementing these patterns are modeled as call activities. We can observe that all Data Subject rights are subject to the so-called "one-month rule", which establishes the maximum time allowed for the Data Controller to fulfill the GDPR obligation. If the request cannot be addressed within 30 days, the Data Controller must provide the Data Subject with a justification for the delay. In BPMN, this is represented by a non-interrupting timer boundary event, enabling the delay notification to be sent without interrupting the ongoing handling of the request. Importantly, if the one-month deadline (extendable to three months in highly complex cases) is not respected, the Data Subject may file a complaint with the Supervisory National Authority, which can impose corrective measures or administrative fines.

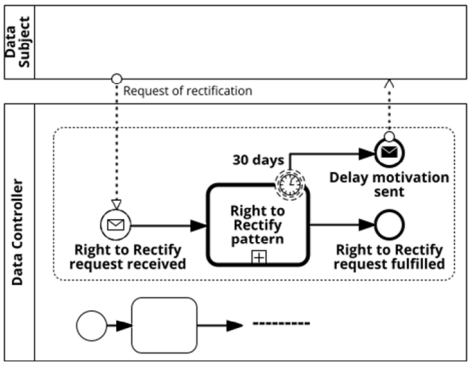
Integrating the GDPR patterns allows the Data Controller to manage all Data Subject requests and respond appropriately to potential data breaches during process execution. If the Data Controller incorporates the relevant patterns as described above, the resulting BPMN model can be considered GDPR-compliant.



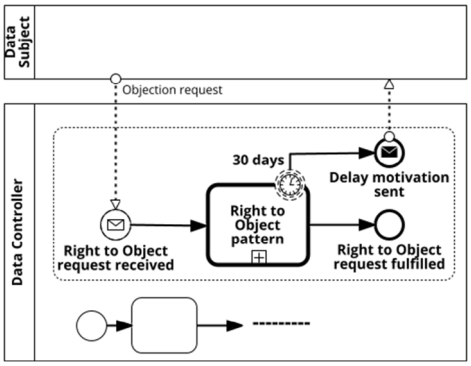
(a) *Right to Access*



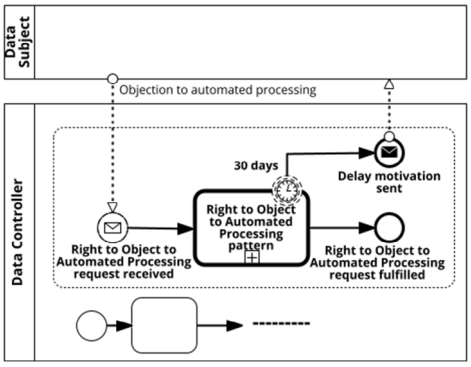
(b) *Right to Portability*



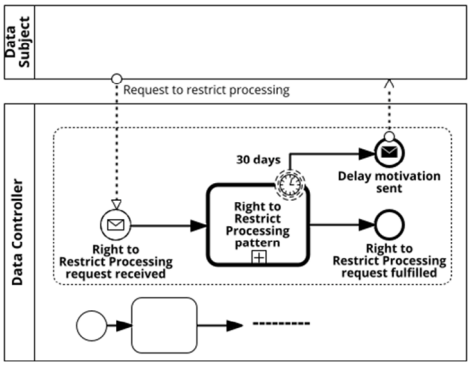
(c) *Right to Rectify*



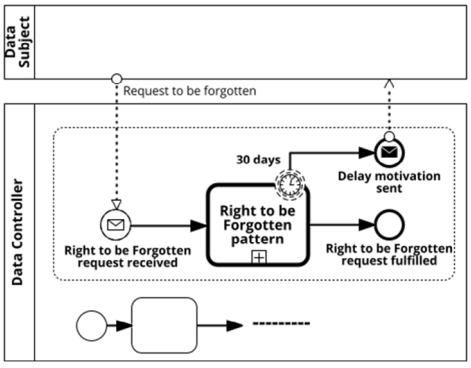
(d) *Right to Object*



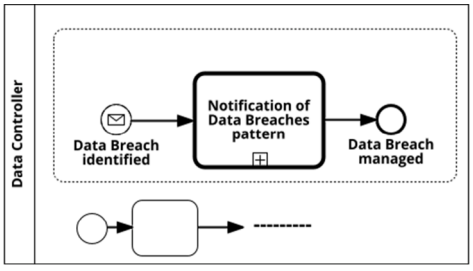
(e) *Right to Object to Automated Processing*



(f) *Right to Restrict Processing*



(g) *Right to be Forgotten*



(h) *Notification of Data Breaches*

Fig. 14. Positioning the GDPR patterns within a process model.

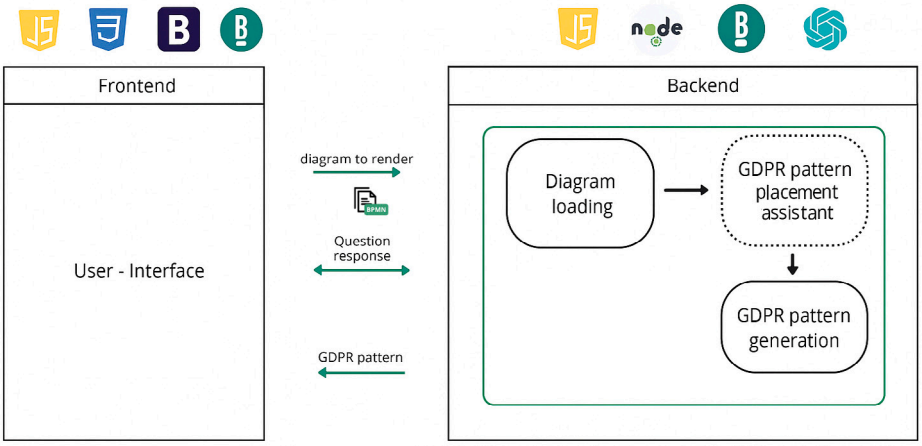


Fig. 15. GDPR-Pilot software architecture.

6.3. GDPR-Pilot: A BPMN editor to incorporate GDPR constraints into BPMN models

The methodology described in Section 6.2 has been implemented in a stand-alone software tool, called GDPR-Pilot, designed to support the transformation of processes into GDPR-compliant models.[11] The tool is available for download at: https://github.com/bpm-diag/GDPR-Pilot. The software architecture devised for GDPR-Pilot is shown in Fig. 15. GDPR-Pilot includes a front-end component with a graphical user interface encoded in HTML5 and the Bootstrap[12] CSS framework, to create a visually appealing and user-friendly interface. It incorporates both the viewer and modeler components from BPMN.io,[13] enabling users to view, create, and edit BPMN processes. This integration ensures that users can interact with BPMN diagrams seamlessly, whether they are visualizing existing processes or designing new ones. Additionally, Webpack[14] is employed to bundle JavaScript modules and static resources, optimizing the performance and efficiency of the front-end.

The back-end component is mainly built with JavaScript and uses the `bpmn-js`[15] and `diagram-js`[16] libraries to work with BPMN.io features. This setup allows for efficient data handling and application logic. Axios is used to make HTTP requests to the OpenAI API,[17] which assists users in identifying when and where GDPR patterns must be included in a process model under analysis. Node.js[18] is used to install and manage all the necessary dependencies. Specifically, the following functionalities are provided:

- **Diagram loading:** The diagram loading feature is executed when the user imports a BPMN diagram into the tool, making the process viewable and editable. It also allows the user to create a new process or to edit an existing one. Fig. 16 presents a screenshot of the tool displaying the BPMN model for the phone company.
- **GDPR pattern placement assistant:** GDPR-Pilot implements the procedure illustrated in Fig. 12 to determine when a GDPR pattern should be incorporated into the BPMN model. As depicted in Fig. 17, the tool provides a side panel that guides the user through a series of GDPR compliance questions, following the sequence outlined in Fig. 12. When the user identifies that specific GDPR obligations need to be represented within the BPMN model, they can select the corresponding activity or activities that trigger those obligations. The tool then automatically inserts the appropriate GDPR patterns into the model at the correct locations, based on the templates illustrated in Figs. 13 and 14. Additionally, GDPR-Pilot includes an optional predictive feature based on LLMs designed to assist users in identifying when a GDPR pattern might be required. This feature leverages OpenAI APIs to generate preliminary suggestions for the GDPR compliance questions shown in Fig. 12, thereby supporting users during the design-time compliance assessment. The current implementation employs the LLM *gpt-3.5-turbo-0125*. It is important to emphasize that the LLM component serves only as a supportive aid; the final decision on whether and where to introduce a GDPR pattern remains entirely with the user. Fig. 17 illustrates how the LLM's suggestions are displayed within the GDPR Panel if the LLM feature is activated. These suggestions are generated using a textual prompt that includes the structure of the uploaded BPMN model, allowing the LLM to identify potential locations where privacy-related constraints may apply. The complete textual prompt is available on the GDPR-Pilot GitHub repository. Further testing is planned to assess the effectiveness of the LLM feature, particularly when handling models with limited or low-quality input data. For this reason, the predictive functionality was deactivated during the expert evaluations described in Section 7.2.2.
- **GDPR pattern generation:** When the user answers a question and the response indicates that a specific GDPR constraint is not met, the tool generates the appropriate pattern to adjust the process accordingly. If the unmet constraint pertains to data consent, the pattern *Consent to Use the Data* is placed as a Call Activity immediately before the activity that does not meet the GDPR constraint. Alternatively, the pattern can be triggered by a start message event and included as part of an event subprocess within the main process, following the logic delineated in Section 6.2.

7. Demonstration and evaluation

To address RQ2, the proposed methodology has been first demonstrated to show its feasibility (cf. Section 7.1) and subsequently evaluated to fulfill the design requirements (cf. Section 7.2). Finally, in Section 7.3, we performed a usability assessment of GDPR-Pilot.

7.1. Demonstration

In this section, we demonstrate the feasibility of our methodology through the phone company use case. Specifically, starting from the

[11] A screencast of the tool is available at the following link: https://youtu.be/2S_3Vj8gRos.
[12] https://getbootstrap.com/
[13] https://bpmn.io/
[14] https://webpack.js.org/
[15] https://github.com/bpmn-io/bpmn-js
[16] https://github.com/bpmn-io/diagram-js
[17] https://openai.com/index/openai-api/
[18] https://nodejs.org/en

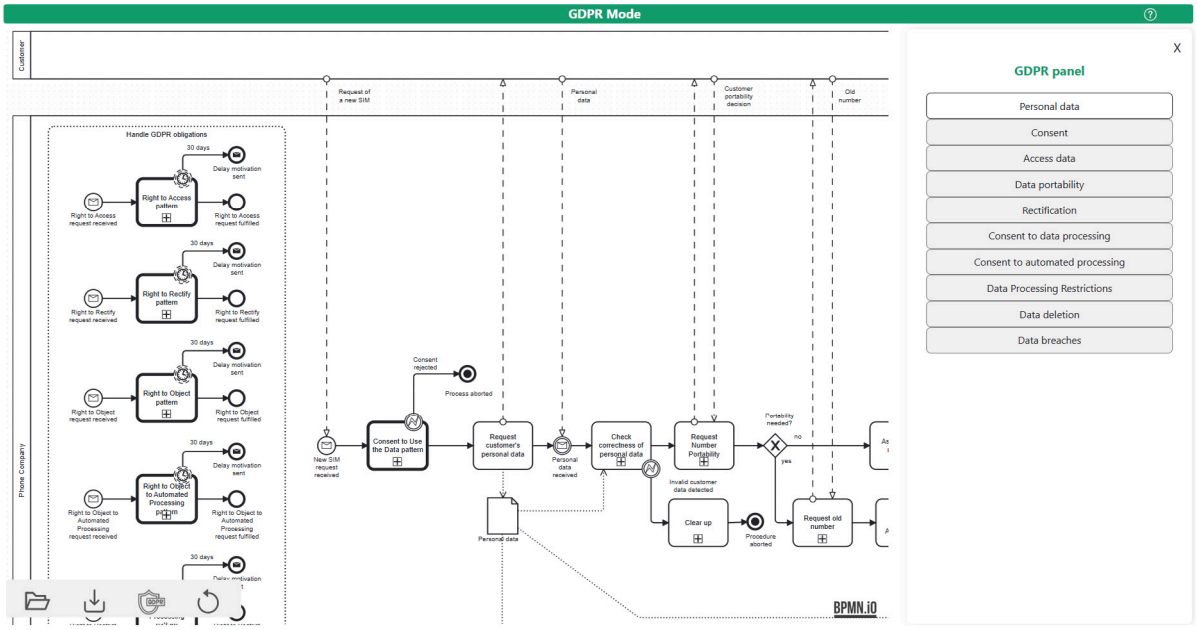


Fig. 16. The phone company process model edited in GDPR-Pilot.

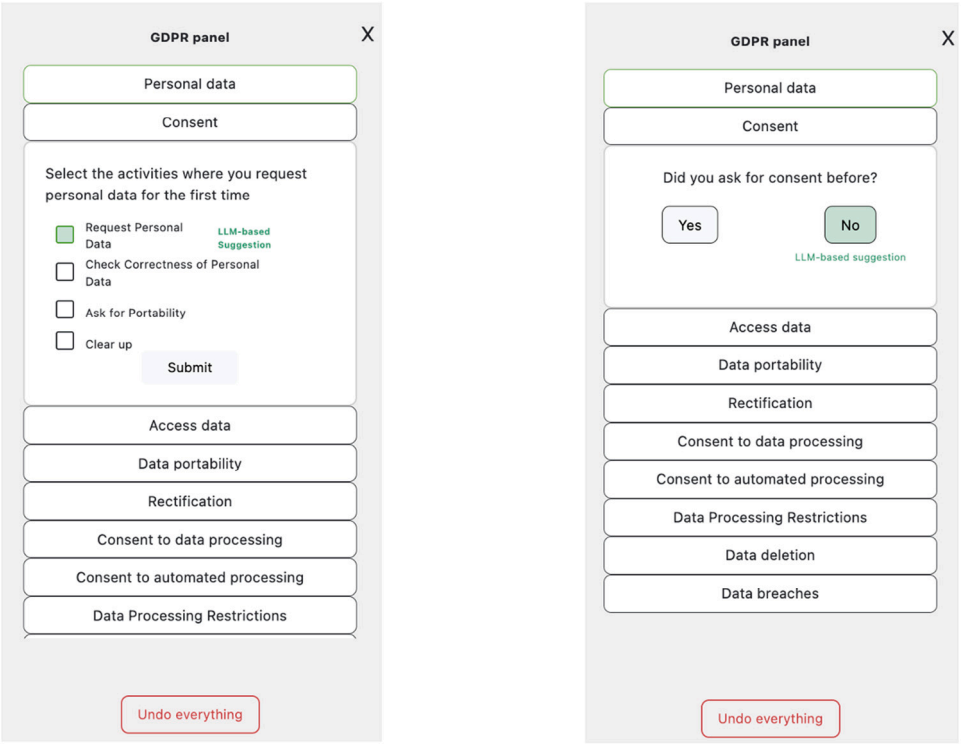


Fig. 17. The GDPR panel displaying LLM predictions.

process model in Fig. 2, which does not comply with the GDPR, we show how our methodology can be applied to produce a GDPR-compliant version of the process model, see Fig. 18.

Following the questions outlined in the procedure depicted in Fig. 12, we first note that performing SIM activation and delivery requires signing a contract, which in turn necessitates the collection of personal data (e.g., name, surname, address, fiscal code, etc.). The BPMN model currently includes an activity labeled "Request customer's personal data". However, to ensure GDPR compliance, the phone company must first obtain the customer's consent to process their personal data. Consequently, the *Consent to Use the Data* pattern (see Fig. 13) is introduced prior to the personal data request activity. Moreover, since personal data is being processed, the *Notification of Data Breaches* pattern (see Fig. 14(h)) must also be applied to the BPMN model to define appropriate mitigation and communication procedures in the event of a data breach (e.g., if an unauthorized access occurs and customer data is exposed during the SIM activation procedure). This ensures that the phone company can promptly notify both the National Supervisory Authority and the affected customers about the breach, detailing its scope, potential impact, and mitigation measures.

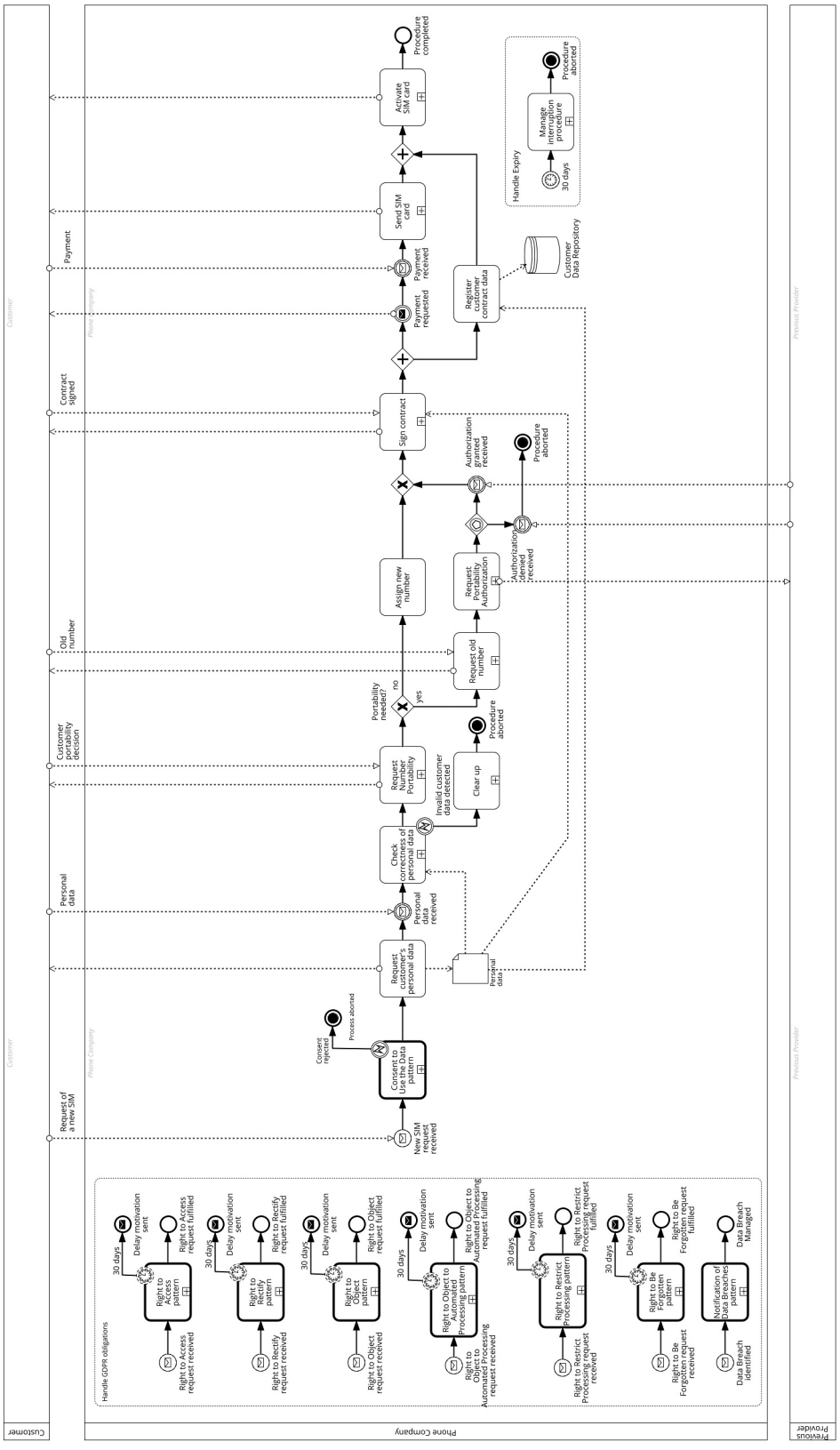


Fig. 18. GDPR-compliant BPMN model for the case of the phone company.

Proceeding with the questions in the methodology of Fig. 12, we can address them as follows:

- **Does the process support Data Subject's right to access their data?** When the customer provides their personal data for the SIM request, those data are collected, stored, and processed across different systems (Customer Relationship Management, billing, logistics, etc.). Therefore, even before the BP is completed (potentially even before the customer signs the contract), integrating the *Right to Access* pattern (see Fig. 14(a)) within the BP guarantees that the customer can transparently verify how their data are being handled.
- **Does the process support Data Subject's right to port their data?** In the BP model of the phone company, the activity labeled "Request portability authorization" represents the company acting as a third-party Data Controller requesting the transfer of personal data from the previous provider. The previous provider, as the original Data Controller, is responsible for implementing the *Right to Data Portability* pattern (see Fig. 14(b)). Consequently, this pattern does not need to be integrated into the BP model of Fig. 2.
- **Does the process support Data Subject's right to rectify their data?** The customer must be able to rectify their personal data at any stage of the SIM activation BP execution, which requires integrating the *Right to Rectify* pattern (see Fig. 14(c)). For instance, if the customer changes address before signing the contract or detects incorrect information, they should have the possibility to correct it.
- **Does the process support Data Subject's right to object the processing of their data?** During the SIM activation BP, the company may use the customer's personal data for marketing purposes. By integrating the *Right to Object* pattern into the BP model (see Fig. 14(d)), the customer can object to such marketing communications. This ensures that the company stops using the customer's data for marketing and allows the rest of the SIM activation BP to continue.
- **Does the process support Data Subject's right to object the automated processing of their data?** The phone company may automatically evaluate a customer's eligibility for a SIM plan using an algorithm that scores creditworthiness or detects potential fraud. By integrating the *Right to Object to Automated Processing* pattern into the SIM activation BP (see Fig. 14(e)), the customer can request human review of decisions made solely by automated processing. This ensures that if the automated decision significantly affects the customer, e.g., a denial of service, the decision can be reviewed, potentially corrected, and justified.
- **Does the process support Data Subject's right to restrict processing of their data?** A customer may dispute the accuracy of their personal data (e.g., an incorrect address) before the SIM is activated. By integrating the *Right to Restrict Processing* pattern into the SIM activation BP (see Fig. 14(f)), the company temporarily limits processing of the disputed data, stopping activities such as billing or marketing, until the issue is resolved. This ensures that the customer's rights are respected while allowing other parts of the SIM activation BP that do not depend on the disputed data to continue.
- **Does the process support Data Subject's right to be forgotten?** A customer may decide to withdraw their subscription request before the SIM is activated. By integrating the *Right to be Forgotten* pattern (see Fig. 14(g)), the company must delete all personal data provided by the customer from the internal databases. This ensures that the customer's data is fully removed and their privacy rights are respected, even if the BP was partially executed and must be aborted due to the unavailability of personal data, preventing the contract from being finalized.

As shown in Fig. 18, with the exception of the *Consent to Use the Data* pattern, all other patterns are embedded within a large event subprocess. This is because they are triggered either by an external message from the customer or, in the case of a data breach, by other entities such as the DPO or the National Authority. We note that, in the appendix, we discuss how two additional use cases (a hiring BP and a healthcare procedure) can be made GDPR compliant by applying our methodology.

7.2. Evaluation

In this section, we provide the evaluation of our artifact by addressing RQ2, thus assessing the requirements listed in Section 5. The evaluation strategy employed was naturalistic since it aims to study phenomena in their natural settings, without artificial manipulations or constraints. Indeed, according to the structure proposed by [21], when conducting a naturalistic evaluation, various approaches can be adopted, such as action research, case study, ethnography, phenomenology, survey, focus group, and participant observation. In this paper, we opted for *participant observation* as the chosen method since it involves participants interacting with the artifact, making decisions in real-world contexts, and solving the designated problems [43]. By adopting participant observation, we were able to understand the users' experiences and behaviors about the artifact's effectiveness.

In light of these considerations, our evaluation was conducted in two steps. First, as described in Section 7.2.1, a preliminary assessment was carried out with 67 MSc students familiar with BPMN. They were asked to transform a non-GDPR-compliant BPMN model into a compliant version by applying the methodology without the support of GDPR-Pilot. Subsequently, in Section 7.2.2, we performed an evaluation with the support of GDPR-Pilot, involving 21 process analysts from the three application domains of our use cases. These experts were asked to analyze the corresponding processes and apply the methodology to transform them into GDPR-compliant models. The collected results were analyzed according to the requirements introduced in Section 5, thus covering structural aspects (*modularity*), usage aspects (*comprehensibility*, *customizability*, and *learnability*), and general environmental aspects (*correctness*).

7.2.1. Preliminary assessment

In the evaluation process, a preliminary assessment with students who had taken the courses of Enterprise Information Systems and Process Management and Mining at the Sapienza University of Rome was performed, as they were familiar with BPMN. The students were provided with a comprehensive list of potential privacy breaches that could occur during the phone company process and asked to redesign it (as described in Section 7.1) to meet privacy violations under the GDPR legislation. The test was conducted on white papers, and the participants were given one hour to complete it. The sample size consisted of 67 students, out of which 54 correctly inserted the patterns and understood both their position and type. The most common errors made by participants were inserting an inappropriate pattern (6 of 13 participants), inserting a pattern in the wrong position (5 of 13 participants), and losing one or more patterns (4 of 13 participants). Some participants (4 of 13) proposed alternative solutions to the provided pattern, which were ineffective in achieving the intended result. These findings suggest that some participants made more than one type of error. Based on the collected results, we evaluated the extent to which the *structural*, *usage* and *generic environmental* introduced in Section 5 were satisfied. The left-hand part of Table 5 summarizes the results of this assessment.

Regarding *structural requirements*, the use of BPMN to specify GDPR patterns enables the representation of process models at multiple levels of abstraction through nested subprocesses. In particular, our methodology allows design patterns to be defined as Call Activities, serving

Table 5
Summary of the evaluation results.

Requirement	Description	Students' assessment	Experts' evaluation
Modularity	Extent to which an artifact can be decomposed into distinct components that may be independently separated, reused, and recombined as required.	GDPR patterns are specified as *Call Activities* in BPMN, representing distinct subprocesses that can be reused across different use case scenarios.	
Comprehensibility	The ease with which an artifact can be understood by a user.	It depends on the users' familiarity with BPMN. The evaluation results, showing that 81% of participants correctly modeled GDPR-aware processes, suggest that most users were able to comprehend the methodology.	The evaluation results, indicating that 85% of participants correctly produced GDPR-aware processes, further substantiate the findings of the students' assessment.
Customizability	The degree to which an artifact can be adapted to the specific needs of local practice.	Partially fulfilled. Certain structural limitations inherent to BPMN may restrict the extent to which patterns can be fully customized to certain cases without compromising compliance.	The methodology was successfully applied across three business domains, showing adaptability to different contexts.
Learnability	The ease with which a user can learn to use an artifact.	It depends on the users' familiarity with BPMN. 81% of participants were able to complete the task in 1 h without any learning issue.	None of the participants: (i) inserted an inappropriate pattern, (ii) placed a pattern incorrectly, or (iii) proposed alternatives to the patterns. The results suggest that the support of GDPR-Pilot facilitates the learnability of the methodology.
Correctness	The extent to which an artifact functions as expected and produces valid outcomes in its intended environment.	$\frac{54\ correct\ GDPR-aware\ process\ models}{67\ process\ models} \simeq 0.81$ 81% of participants model GDPR-aware processes correctly.	$\frac{18\ correct\ GDPR-aware\ process\ models}{21\ process\ models} \simeq 0.85$ 85% of participants model GDPR-aware processes correctly.

as reusable building blocks that can be flexibly integrated into different processes while preserving separation from domain-specific logic. This capability inherently facilitates the achievement of *modularity* by design.

Concerning the *environmental requirements*, observations of the participants indicate that 54 out of 67 students were able to correctly insert the patterns and accurately identify their position and type within the BPMN model. In this context, *correctness* implies that a process model, once augmented with GDPR patterns, accurately complies with the GDPR regulatory requirements. Calculating correctness as the ratio of correct results (i.e., the number of users who successfully converted non-compliant BPMN models using our methodology) to total results (i.e., all users) yields an overall correctness of approximately 81%. It is important to note that this measure is conservative, as participants who only partially enhanced the BPMN models in a correct way were counted as incorrect results.

With regard to the *usage requirements*, the use of BPMN as the modeling notation for specifying the design patterns inherently supports these requirements. In particular, *comprehensibility* requires that GDPR patterns are represented in a manner that makes their purpose and compliance function immediately clear to users. Since the patterns are expressed using standard BPMN constructs without requiring any extensions, and modifications to a non-GDPR-compliant model are implemented as simple Call Activities, the comprehensibility of the methodology largely depends on the users' familiarity with BPMN. Consequently, we can conclude that the comprehensibility of the methodology is closely correlated with the end-user's experience with BPMN. Similar considerations apply to *learnability*, which requires that GDPR patterns be designed so that new users can readily understand how to apply and reuse them correctly. The evaluation results, with 81% of participants successfully modeling GDPR-aware BPMN processes, indicate that at least 81% of users were able to *comprehend* the methodology and successfully *learn* its mechanisms within the one-hour time frame provided for the test.

Finally, regarding *customizability*, this requirement reflects the need for patterns to be adaptable to the specific organizational and contextual variations of GDPR obligations, while preserving their underlying compliance structure. Based on the students' observations, our impression was that this requirement is only partially fulfilled by our methodology. On the one hand, since GDPR patterns are defined using standard BPMN constructs, users can adapt their behavior to fit specific application scenarios. On the other hand, certain structural limitations inherent to BPMN may restrict the extent to which patterns can be customized without compromising compliance.

7.2.2. Evaluation with domain experts

To provide a more precise assessment of requirement satisfaction, we conducted a second round of evaluation involving 3 clusters of users: 8 employees from the telecommunications sector, 8 from corporate hiring, and 5 from healthcare administration, corresponding to the three use cases employed in this paper, related to a SIM activation process (cf. Fig. 2), a hiring process (cf. Fig. A.19), and an healthcare procedure (cf. Fig. A.21). The participants were carefully selected to ensure expertise in BPMN and familiarity with implementing GDPR policies in their respective companies. Each evaluation session was conducted separately in an online setting. To avoid requiring participants to install the tool on their own devices, they were granted remote access to a dedicated workstation where the tool was pre-installed and running. Each user received initial instruction on the functionalities of GDPR-Pilot (cf. Section 6.3) through a brief training session, followed by an interactive session using the tool.

Participants in each cluster were provided with a list of potential privacy breaches specific to their respective processes and were asked to redesign these processes using GDPR-Pilot to ensure compliance with the GDPR. GDPR-Pilot, through its GDPR pattern placement assistant component, guided each expert through the methodology presented in Fig. 12, prompting them (question by question) about potential GDPR non-compliance and automatically inserting the appropriate patterns in the correct locations when requested by the user. Participants were given one hour to complete the task. It should be noted that, during this round of evaluation, the LLM-based predictive feature of the GDPR pattern placement assistant was intentionally deactivated to ensure that the study focused exclusively on human-driven decisions.

The results of the evaluation show that 100% of participants (21 in total) did not: (i) insert an inappropriate pattern, (ii) place a pattern incorrectly, or (iii) propose any alternative solution to the provided pattern, in contrast to the preliminary student assessment. This difference can be attributed to the use of GDPR-Pilot, which constrains the modifications to the BPMN model within the scope of the predefined patterns, thereby guiding users toward consistent and correct application. In

summary, the second round of evaluation confirms that participants were able to redesign the processes within one hour, indicating that the methodology is relatively *easy to learn*.

Nonetheless, 3 out of 21 participants (one per cluster) omitted one or more patterns when responding to GDPR-related question. Consequently, 18 out of 21 participants (87.5% for the SIM activation process, 87.5% for the hiring process, and 80% for the healthcare procedure) successfully produced GDPR-aware process models that adhered to the correct GDPR-enhanced version (cf. Figs. 18, A.20, and A.22), corresponding to an average *correctness* of 85%, which confirms and substantiates the positive outcome of the preliminary assessment.

Moreover, the fact that, on average, 85% of participants produced correct GDPR-aware BPMN models suggests that most users were able to *comprehend* our methodology, thereby reinforcing the 81% result obtained in the preliminary evaluation. Regarding *customizability*, although no definitive conclusions can be drawn, the results are noteworthy, as the methodology was successfully applied across three distinct business domains, demonstrating its potential adaptability to different contexts. Finally, no additional observations can be made concerning *modularity*, as this property is entirely inherent to BPMN.

7.3. Quantifying the usability of GDPR-Pilot

We measured the usability of GDPR-Pilot through a SUS (System Usability Scale) questionnaire involving the aforementioned cluster of 21 expert users. At the conclusion of the second round of evaluation, users were administered with a 10-item SUS questionnaire, which rates responses on a five-point Likert scale [44] from *1-strongly disagree* to *5-strongly agree*. The ten questions of the SUS are reported in the following:

- q1. I think that I would use GDPR-Pilot frequently;
- q2. I found GDPR-Pilot unnecessarily complex;
- q3. I thought GDPR-Pilot was easy to use;
- q4. I think that I would need the support of a technical person to be able to use GDPR-Pilot;
- q5. I found the various functions of GDPR-Pilot were well integrated;
- q6. I thought there was too much inconsistency in GDPR-Pilot;
- q7. I would imagine that most people would learn to use GDPR-Pilot very quickly;
- q8. I found GDPR-Pilot very awkward to use;
- q9. I felt very confident using GDPR-Pilot;
- q10. I need to learn a lot of things before I could get going with GDPR-Pilot.

The overall SUS score (cf. [22] for instructions on how to compute it), considered a reliable measure of perceived usability and user experience, was benchmarked against literature standards to determine GDPR-Pilot's usability. The average SUS score was 83.6 (cf. Table 6), corresponding to an *A rank* according to the selected benchmark [22], indicating an excellent usability of the tool.

8. Conclusion and future works

The enforcement of GDPR has profoundly impacted the way organizations design and manage business processes, requiring effective strategies to address privacy concerns. This paper presents a methodology for developing GDPR-aware business processes directly at design-time, rather than intervening only at run-time when breaches occur. Our systematic approach guides process designers and Data Controllers in integrating GDPR patterns at precise points in the process model, thereby anticipating and preventing potential privacy violations across all process instances. Compared to state-of-the-art approaches, the key advantage of our methodology is the use of design patterns that embed GDPR principles without extending BPMN. This ensures compliance can be verified directly at design-time and guarantees compatibility with any BPMS supporting standard BPMN. By contrast, existing methods rely on custom extensions, which impose additional learning burdens on designers and require modifications to BPMSs to interpret the extended notation. To support Data Controllers in applying our methodology and deciding when each pattern should be used, we developed GDPR-Pilot, a BPMN editor that semi-automatically assists process designers in integrating the patterns into existing models. Finally, we evaluated our methodology on real-world use cases against structural, usage, and environmental requirements, both without and with the support of the tool, to demonstrate its effectiveness.

The use of BPMN is a strength of our methodology, as it ensures modularity by design. Indeed, patterns are defined as reusable building blocks that can be flexibly integrated into different business processes while remaining separate from domain-specific logic. With only a basic understanding of BPMN constructs, the methodology can be considered both easy to learn and comprehensible, as also discussed in Section 7. The evaluation further showed that users were able to create correct GDPR-aware models with relatively little effort. On the other hand, while the application of the methodology to three use cases in different domains suggests its potential generalizability, certain structural limitations inherent to BPMN may restrict the extent to which patterns can be fully customized for ad-hoc situations without compromising compliance. We plan to investigate this aspect further by conducting a larger evaluation involving additional GDPR experts, asking them to modify the predefined patterns with ad-hoc policies in order to assess the extent to which our BPMN-based methodology can adequately capture such customized policies. This may also involve a comparative study with other state-of-the-art approaches to evaluate and contrast their ability to capture ad-hoc constraints.

Another limitation that requires further investigation concerns the quality of the process models provided as input to the methodology. When the management and processing of personal data are represented by activities with ambiguous or unclear names, identifying the appropriate privacy patterns to apply can become more challenging. The use of GDPR-Pilot (particularly the LLM-based features integrated into the GDPR pattern placement assistant) has the potential to mitigate this issue, as also evidenced by recent works that exploit LLMs to support semi-automated process modeling with BPMN [45,46]. However, since the LLM feature was deactivated and therefore not included in the evaluation performed in this paper, we plan to conduct additional future testing to assess the effectiveness of the LLM feature in supporting users working with low-quality input models, compared to scenarios in which the feature is not used.

CRediT authorship contribution statement

Simone Agostinelli: Writing – original draft, Project administration, Methodology, Investigation, Formal analysis, Conceptualization. **Francesca De Luzi:** Visualization, Resources, Data curation. **Fabrizio Maria Maggi:** Writing – original draft, Investigation, Conceptualization. **Andrea Marrella:** Writing – original draft, Supervision, Investigation, Funding acquisition, Formal analysis, Conceptualization. **Alessia Volpi:** Visualization, Validation, Software, Formal analysis.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgments

This work was supported by the Sapienza project FOND-AIBPM, the PRIN 2022 project MOTOWN, and the PNRR MUR project PE0000013-FAIR. We would like to thank all the colleagues who have contributed to this line of research over the years through their comments and feedback, particularly Martina Ligi and Anna Maria Fiorentino.

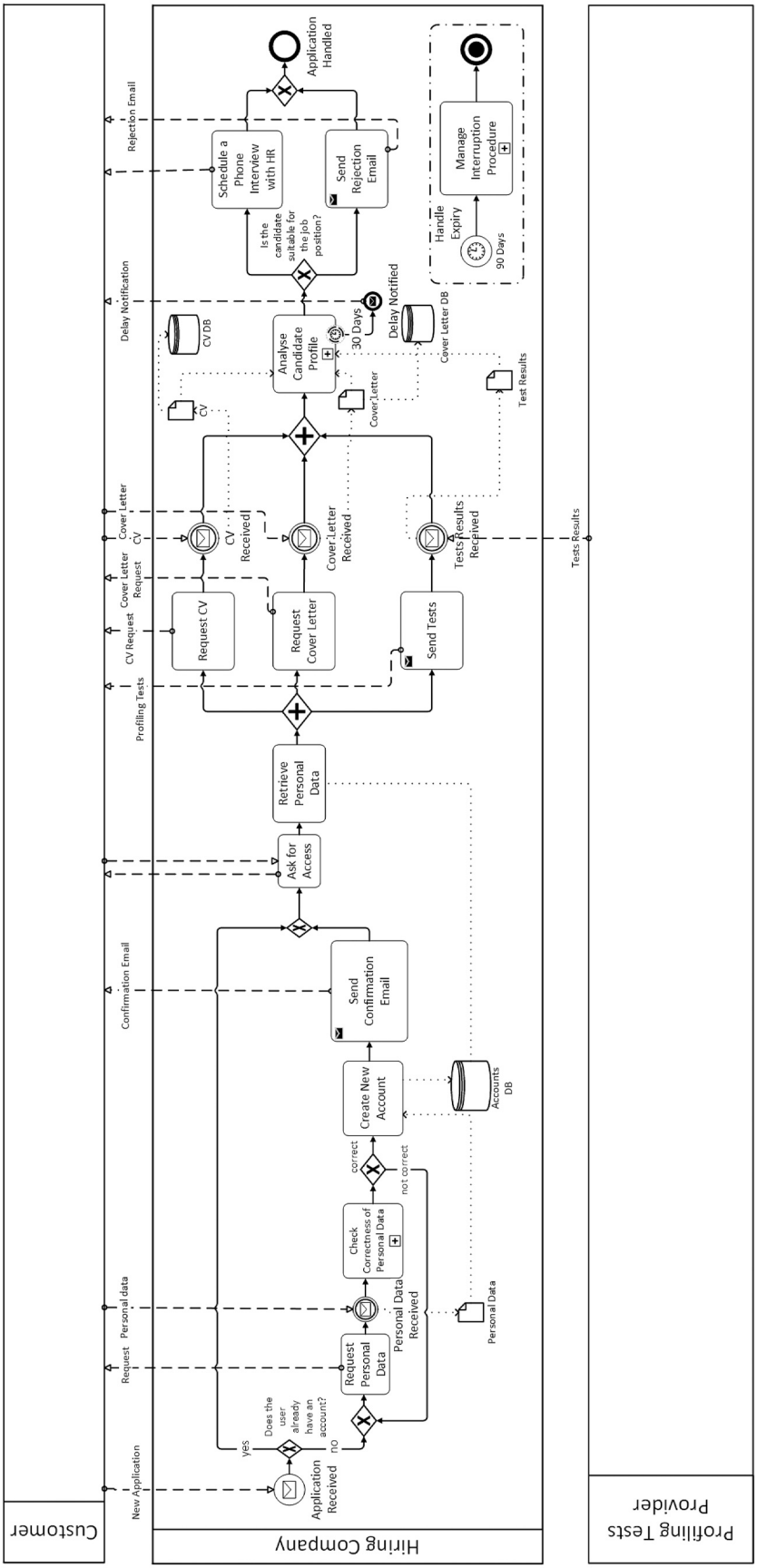


Fig. A.19. BPMN model for the case of the hiring company.

Table 6
Computation of the SUS overall score.

User	q1	q2	q3	q4	q5	q6	q7	q8	q9	q10	SUS score	Average
p1	4	2	5	2	5	1	3	2	3	2	77.5	83.6
p2	5	1	5	1	5	1	4	1	3	1	92.5	
p3	4	2	4	2	4	2	3	2	4	2	72.5	
p4	5	1	5	1	5	1	3	1	3	1	90.0	
p5	5	2	5	1	4	1	3	2	3	2	80.0	
p6	4	2	4	2	5	1	3	2	3	1	77.5	
p7	5	1	5	1	5	2	4	1	5	2	92.5	
p8	5	2	5	2	4	1	3	2	3	1	80.0	
p9	5	1	5	1	5	1	3	1	3	2	87.5	
p10	5	1	5	1	5	2	3	1	4	1	90.0	
p11	4	2	4	2	4	1	3	2	5	2	77.5	
p12	5	1	5	1	5	2	4	1	4	1	92.5	
p13	5	1	5	1	5	1	3	2	3	2	85.0	
p14	4	2	4	2	4	2	3	1	3	1	75.0	
p15	5	1	5	1	5	1	3	2	3	2	85.0	
p16	5	1	5	1	5	2	3	2	5	1	90.0	
p17	4	2	4	2	4	1	4	1	3	2	77.5	
p18	5	1	5	1	5	2	3	2	3	1	85.0	
p19	5	2	5	1	5	1	3	1	4	2	87.5	
p20	4	1	4	2	4	2	3	2	4	1	77.5	
p21	4	2	5	1	5	2	3	1	4	2	82.5	

Appendix

The BPMN model in Fig. A.19 represents a generic *hiring company* receiving an application request for a job position. The process starts when someone applies for the position. If the applicant has an active account, the company asks them to log in with their credentials. Otherwise, the company asks the user for their data (e.g., name, surname, email address, phone number). Once the data is verified (and corrected if needed), the company creates an account and sends a confirmation email. After that, the applicant can log in with the new credentials. Once the user is logged in, the hiring company retrieves the applicant's data and asks the applicant to send a CV and Cover Letter. CV and Cover Letter are then stored in a database that the recruiter will access later on in the process. In the meantime, the company sends the applicant a set of personality, behavioral, and ability tests to complete at their convenience. Such tests will be then analyzed by a profiler and the results will support the recruiter in the evaluation. A phone interview is scheduled if the applicant is deemed suitable for the job position. Otherwise, a rejection email is sent. In either case, the hiring procedure is complete. If, for some reason, the procedure takes more than 3 months to complete, then the process is interrupted and the application will not be taken into consideration. Finally, please note that the exchange of personal data does not imply proper handling of personal data in accordance with the GDPR regulation.

In the following, we show how applying the methodology to the use case enables the transformation of the process model that is not compliant with GDPR in its compliant counterpart.

The BPMN model provided above does not take into account privacy concerns yet, thus, after the coming into effect of GDPR, on 25 May 2018, if the company has to evaluate the profile of a candidate located in the EU, the whole process model has to be modified to become GDPR compliant. Since personal data are processed and need to be retrieved, it is mandatory to obtain the data subject's consent for their processing. Therefore, the process designer needs to add a request for consent to the model, as consent has not yet been given. Such a request has to be provided to the user together with a list of privacy information, so that the applicant is informed about how data will be processed, by whom, and for what purpose. Consent and privacy information are included in the pattern *Right to Be Informed and to Consent*, which has to be placed before the first request for personal data occurs. In this case, the three PIIs identified in the model are the personal data such as name, surname, birth date, address, etc., the CV, and the test results provided to the hiring company by a test provider in the form of an applicant's profile. During the execution of the process, the first activity that requests personal data is the one associated with the filling module for personal data during the creation of a new account. At this moment, the pattern should be introduced and it should include consent for all future requests for personal data. In fact, it makes sense that consent is requested when a new account is created, thus for any future job application, consent has already been provided and data can be retrieved more easily. If a data breach occurs during the hiring process (e.g., unauthorized access to CVs stored in the recruitment system), the *Notification of Data Breaches* pattern must also be applied to the BPMN model, ensuring that both the National Supervisory Authority and the affected applicants are notified within 72 h, with details on scope, risks, and mitigation measures.

The GDPR-compliant BPMN model for the hiring procedure is illustrated in Fig. A.20. Proceeding with the questions in the methodology of Fig. 12, we can address them as follows:

- **Does the process support Data Subject's right to access their data?** Applicants may request access to their submitted CVs and personal data at any stage of the hiring process, thus the *Right to Access* pattern should be integrated as an event subprocess and should be executable at any moment. The HR department collects all relevant data, prepares an access report (e.g., stored CV, interview notes, and evaluation results), and provides it to the applicant.
- **Does the process support Data Subject's right to port their data?** A candidate could request that their application data be transferred to another recruitment agency. However, the responsibility for implementing the *Right to Data Portability* pattern lies with the receiving organization, and thus this pattern is not integrated into the hiring process model.
- **Does the process support Data Subject's right to rectify their data?** The applicant must be able to rectify their personal data at any stage of the process execution, which requires integrating the *Right to Rectify* pattern. For instance, if the candidate updates their phone number, address, or provides a new version of their CV, they should have the possibility to modify the stored information.
- **Does the process support Data Subject's right to object the processing of their data?** During the recruitment process, the company may use applicant data for additional purposes (e.g., future job offers). By integrating the *Right to Object* pattern into the hiring process model, the applicant can object to such processing, ensuring their data is only used for the ongoing selection procedure.

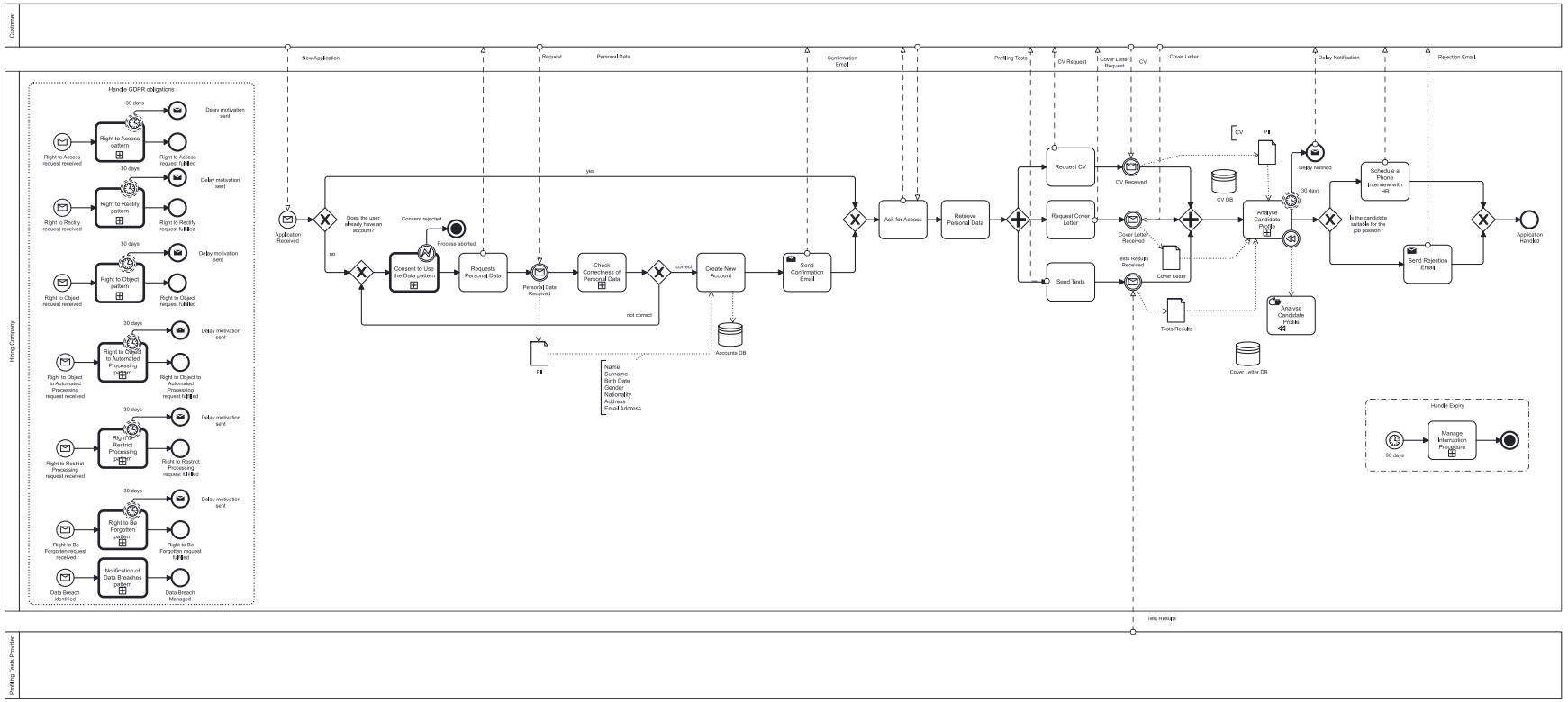


Fig. A.20. GDPR-compliant BPMN model for the case of the hiring company.

- **Does the process support Data Subject's right to object the automated processing of their data?** Hiring procedures may involve automated pre-screening tools that filter CVs or rank applicants using algorithms. Since such automation may significantly affect candidates (e.g., rejection before human evaluation), by integrating the *Right to Object to Automated Processing* pattern, the applicant can request human review of decisions made solely by automated systems. To ensure the execution of the pattern, every activity taking a decision based on automated mechanisms must dispose of a compensation handler, enabling human intervention in the decision. This is what has been done with the activity "Analyze Candidate Profile", whose compensation activity is the manual activity named "Analyze Candidate Profile" as well.
- **Does the process support Data Subject's right to restrict processing of their data?** An applicant may dispute the accuracy of some submitted information or request limitation of processing during a background check. By integrating the *Right to Restrict Processing* pattern, the company temporarily limits processing of the disputed or sensitive data until the problem is resolved, while other non-affected process activities may continue.
- **Does the process support Data Subject's right to be forgotten?** If a candidate is not hired, they may request the deletion of their data after the recruitment process is completed. Consequently, by integrating the *Right to Be Forgotten* pattern, the company deletes all personal data (e.g. CVs, ratings, interview notes) once the retention period has expired, unless consent has been obtained explicit for longer storage.

The BPMN model in Fig. A.21 represents a healthcare process from the cardiology department of a hospital, involving the evaluation and preparation of patients undergoing potential cardiac surgery [47,48]. The model captures the interaction among different roles: patient, nurse, physician, administrative and diagnostic staff. A new process instance is instantiated whenever a patient is referred for surgery. Initially, an administrative clerk collects a range of personal information and a nurse admits the patient, collecting medical history (e.g., allergies, comorbidities, previous treatments), and updates the patient's record. This information is recorded in the hospital's electronic health system. Following data acquisition, a physician performs a preliminary evaluation and the patient is scheduled for a series of diagnostic procedures, that are carried out by external laboratories (often supported by robotic automation). With the notes from the examination and the blood analysis results, the physician has to make a diagnosis. Based on the results, a surgical intervention is either immediately performed by the physician or it is planned for the following days by the nurse, keeping in mind that the patient may also refuse to undergo surgery. In all cases, the patient is discharged while being provided with discharge documents and the administration updates the patient's record concurrently. After discharge, the administration invites the patient to access a hospital-managed digital portal to download medical documentation and provide optional feedback on the care received. The portal integrates third-party analytics tools to monitor user behavior (e.g., page visits, session time, device data) and to suggest targeted health-related content, such as follow-up programs, lifestyle recommendations, or insurance offers.

In the following, we show how applying the methodology to the use case enables the transformation of the process model that is not compliant with the GDPR in its compliant counterpart.

Since several categories of personal data are processed, stored, and exchanged among actors within and outside the hospital, it becomes mandatory to obtain explicit and informed consent from the patient for data processing activities. Consequently, the BPMN model has to include a specific activity where the patient is informed about data processing, and where a patient's consent is requested and recorded. This consent must be obtained before any data acquisition occurs. Consent and privacy information are included in the pattern *Right to Be Informed and to Consent*, which has to be placed before the first request for personal data occurs. In this case, the first such activity is the collection of personal and medical information by the administrative clerk and the nurse. Therefore, the BPMN model must be modified to include an activity that presents the patient with privacy information, such as purpose of processing, legal basis, retention periods, recipients (e.g., external laboratories), and rights, along with a request for consent. Moreover, as the process handles sensitive health information, the *Notification of Data Breaches* pattern must be incorporated. This ensures that both the National Supervisory Authority and the affected patients are notified, specifying the nature and consequences of the breach. Proceeding with the questions in the methodology of Fig. 12, we can address them as follows:

- **Does the process support Data Subject's right to access their data?** Patients may request access to their medical records at any stage, thus the *Right to Access* pattern should be integrated as an event subprocess and should be executable at any moment. The hospital collects all relevant data, prepares an access report, and provides it to the patient.
- **Does the process support Data Subject's right to port their data?** Upon discharge, the patient could also request that their data be transferred to another hospital, with the purpose of allowing patients to exchange and provide access to their primary health data processed by public or private controllers between multiple healthcare professionals. The new hospital is responsible for implementing the *Right to Data Portability* pattern.
- **Does the process support Data Subject's right to rectify their data?** The patient must be able to rectify their personal data at any stage of the process execution, which requires integrating the *Right to Rectify* pattern. For instance, if the patient detects errors in their medical data (e.g., wrong address, incorrect personal information), they should have the possibility to correct it.
- **Does the process support Data Subject's right to object the processing of their data?** During the processing of health data collected by internal and external hospital staff, the hospital may use the patient's personal data for purposes other than processing (e.g., suggestion of content). By integrating the *Right to Object* pattern into the process model, the patient can object to such communications. This does not affect the lawfulness of the preventive treatment.
- **Does the process support Data Subject's right to object the automated processing of their data?** Although the healthcare process as modeled does not explicitly include automated decision-making, it should be noted that in the internal laboratory workflow advanced automation and robotization systems are foreseen. These systems significantly improve efficiency in resource management, guarantee continuous traceability of samples, accelerate both pre-analytical and analytical phases, provide faster availability of results, and enhance the safety of laboratory staff. Since such automation may directly affect patients by influencing the reliability of diagnostic outcomes, by integrating the *Right to Object to Automated Processing* pattern the patient can request human review of decisions made solely by automated processing.
- **Does the process support Data Subject's right to restrict processing of their data?** A patient has the right to limit the processing of personal health data in specific situations, for example when he disputes the accuracy of the data (e.g., an incorrect address). By integrating the *Right to Restrict Processing* pattern, the hospital temporarily limits processing of the disputed data until the problem is resolved.
- **Does the process support Data Subject's right to be forgotten?** The 2019 annual report[19] of the Italian Guarantor for the

[19] https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9427952

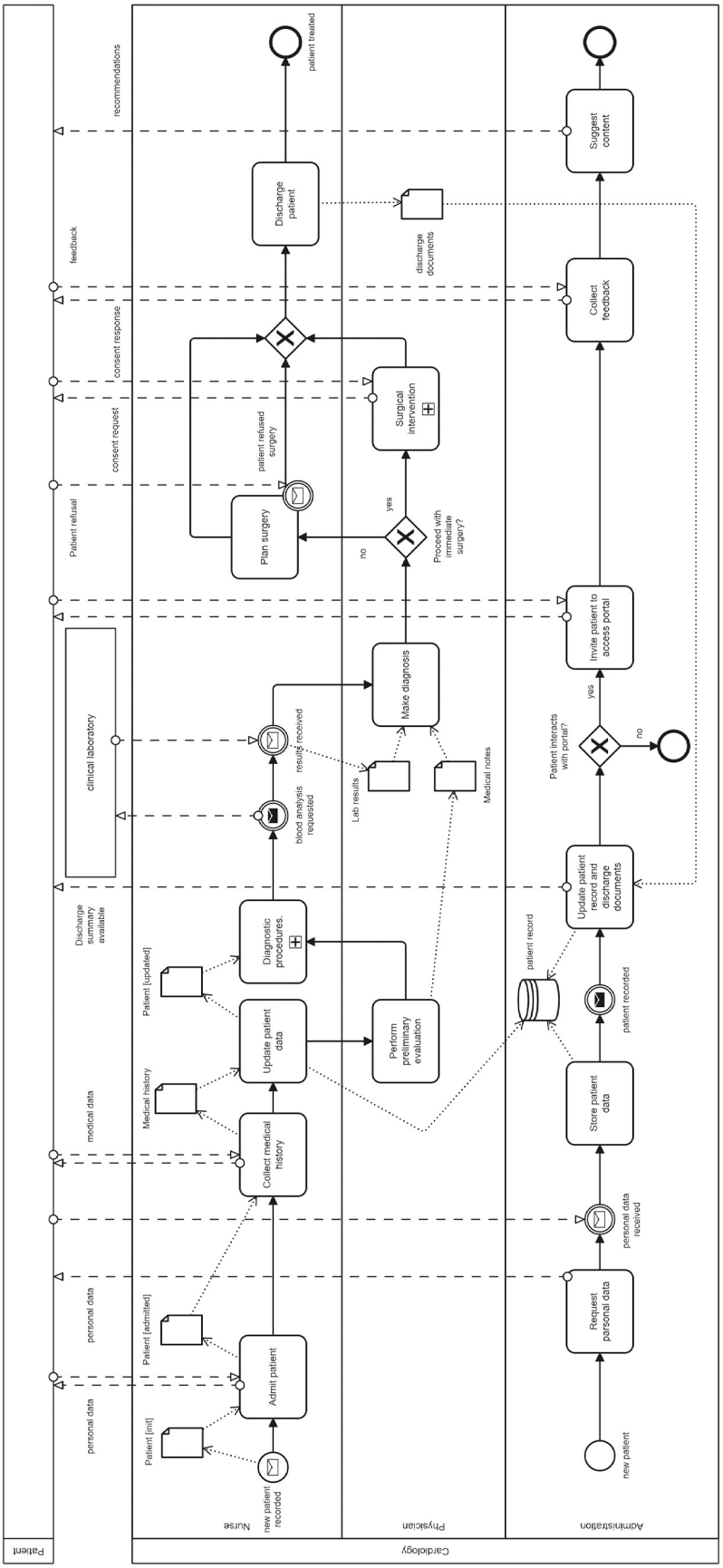


Fig. A.21. BPMN model for the case of the surgery process.

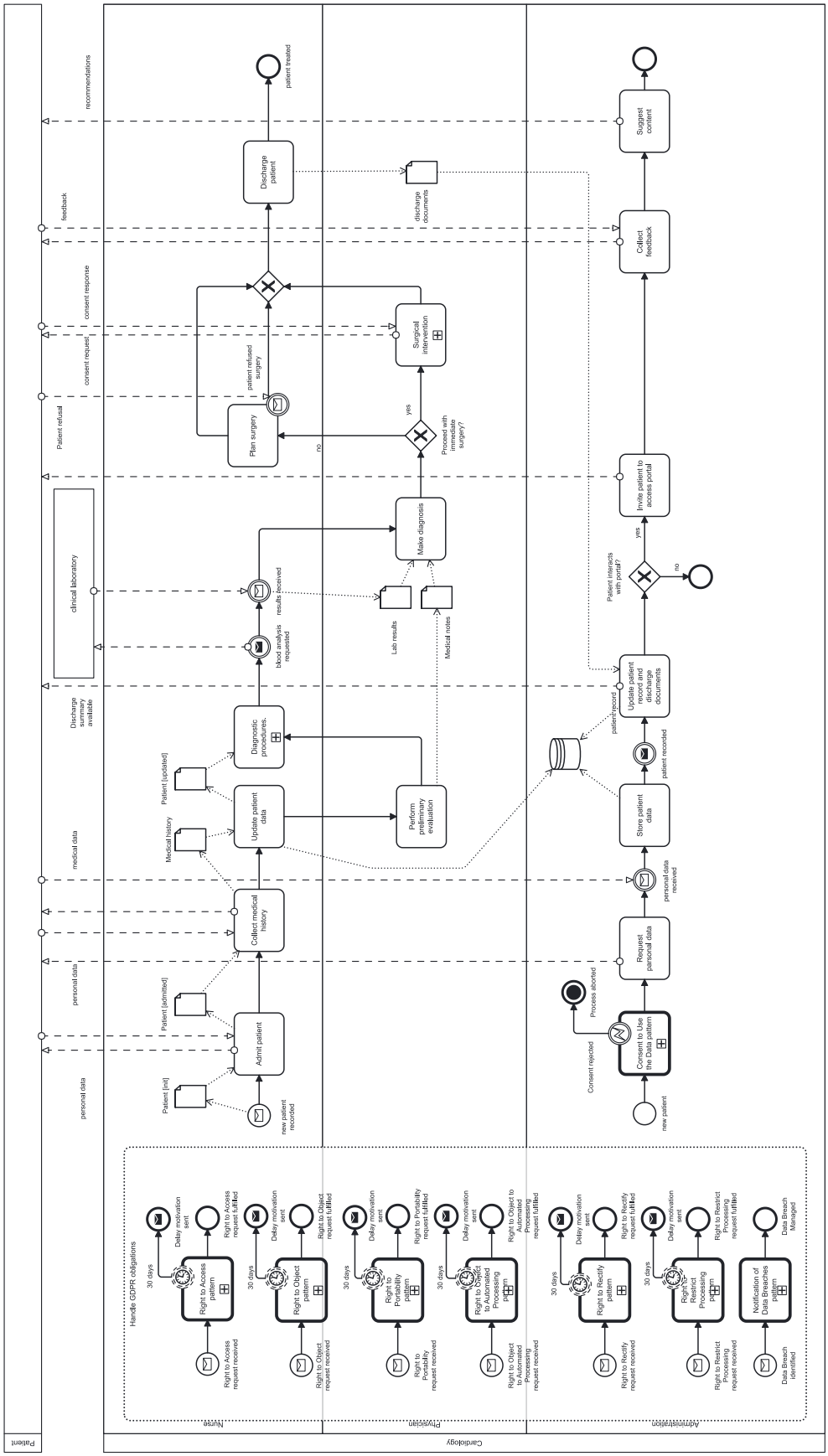


Fig. A.22. GDPR-compliant BPMN model for the case of the surgery process.

protection of personal data highlights how the personal data contained in the medical records cannot be deleted, as only their rectification or integration is permitted, and this is because the medical record must be considered as a public document, aimed at faithfully certifying, up to a complaint of falsification and in the interest of all parties involved, specific clinical and therapeutic choices and, as such, is capable of producing effects on multiple subjective legal situations. Consequently, the *Right to Be Forgotten* pattern does not need to be integrated into the process model of Fig. A.22.

Data availability

Data will be made available on request.

References

[1] S.A. Petersen, F. Mannhardt, M. Oliveira, H. Torvatn, A Framework to Navigate the Privacy Trade-offs for Human-Centred Manufacturing, in: 19th IFIP Conf. on Virt. Enterprises, Springer, 2018.

[2] D. Basin, S. Debois, T. Hildebrandt, On purpose and by necessity: compliance under the GDPR, in: 22th Int. Conf. on Financial Cryptography and Data Security, Springer, 2018.

[3] A. Capodieci, L. Mainetti, Business Process Awareness to Support GDPR Compliance, in: 9th Int. Conf. on Information Systems and Technologies, ICIST'19, ACM, 2019.

[4] M. Dumas, M. La Rosa, J. Mendling, H.A. Reijers, Fundamentals of Business Process Management, Springer, 2018.

[5] M. Weske, Business Process Management. Concepts, Languages, Architectures, Springer, 2024.

[6] P. Pullonen, R. Matulevicius, D. Bogdanov, PE-BPMN: Privacy-Enhanced Business Process Model and Notation, in: 15th Int. Conf. on Business Process Management (BPM'17), Springer, 2017.

[7] S. Belluccini, R. De Nicola, M. Dumas, P. Pullonen-Raudvere, B. Re, F. Tiezzi, Model-based verification of data protection mechanisms in collaborative business processes, Softw. Syst. Model. 24 (2) (2025) 489–521.

[8] Á.J. Varela-Vaca, M.T. Gómez-López, Y. Morales Zamora, R. M. Gasca, Business process models and simulation to enable GDPR compliance, Int. J. Inf. Secur. 24 (1) (2025) 41.

[9] S. Agostinelli, F.M. Maggi, A. Marrella, F. Sapio, Achieving GDPR compliance of BPMN process models, in: 31st Int. Conf. on Advanced Information Systems - CAiSE Forum 2019, vol. 350, Springer, 2019, pp. 10–22.

[10] R. Matulevičius, J. Tom, K. Kala, E. Sing, A Method for Managing GDPR Compliance in Business Processes, in: International Conference on Advanced Information Systems Engineering, Springer, 2020, pp. 100–112.

[11] M. Menzel, I. Thomas, C. Meinel, Security Requirements Specification in Service-Oriented Business Process Management, in: 4th Int. Conf. on Availability, Reliability and Security, IEEE, 2009.

[12] Y. Cherdantseva, J. Hilton, O.F. Rana, Towards SecureBPMN - Aligning BPMN with the Information Assurance and Security Domain, in: 4th Int. Workshop on BPMN, Springer, 2012.

[13] G.B. Ayed, S. Ghernaouti-Helie, Processes View Modeling of Identity-related Privacy Business Interoperability: Considering User-Supremacy Federated Identity Technical Model and Identity Contract Negotiation, in: Int. Conf. on Adv. in Social Net. Analysis and Mining, IEEE, 2012.

[14] O. Altuhhova, R. Matulevicius, N. Ahmed, An Extension of Business Process Model and Notation for Security Risk Management, Int. J. Inf. Syst. Model. Des. 4 (4) (2013).

[15] A.D. Brucker, Integrating Security Aspects into Business Process Models, Inf. Tech. 55 (6) (2013).

[16] W. Labda, N. Mehandjiev, P. Sampaio, Modeling of privacy-aware business processes in BPMN to protect personal data, in: Symposium on Applied Computing, SAC'14, ACM, 2014.

[17] M. Salnitri, F. Dalpiaz, P. Giorgini, Designing secure business processes with SecBPMN, Softw. Syst. Model. 16 (3) (2017).

[18] C. Bartolini, A. Calabró, E. Marchetti, GDPR and business processes: An effective solution, in: 2nd Int. Conf. on Applications of Intelligent Systems, APPIS '19, ACM, 2019.

[19] S.I. Besik, J.-C. Freytag, Managing consent in workflows under GDPR., in: ZEUS, 2020, pp. 18–25.

[20] D. Granata, M. Rak, G. Salzillo, G. Di Guida, S. Petrillo, Automated threat modelling and risk analysis in e-Government using BPMN, Connect. Sci. 35 (1) (2023) 2284645.

[21] P. Johannesson, E. Perjons, An Introduction to Design Science, Springer, ISBN: 978-3-319-10632-8, 2014, pp. 1–193.

[22] J. Sauro, J.R. Lewis, Quantifying the User Experience: Practical Statistics for User Research, Morgan Kaufmann, 2016, http://dx.doi.org/10.1145/2413038.2413056.

[23] A. Marrella, M. Mecella, B. Pernici, P. Plebani, A design-time data-centric maturity model for assessing resilience in multi-party business processes, Inf. Syst. 86 (2019) 62–78.

[24] F. De Luzi, F. Leotta, A. Marrella, M. Mecella, On the Interplay Between Business Process Management and Internet-of-Things, Bus. Inf. Syst. Eng. 67 (2025).

[25] C.L. Maines, D. Llewellyn-Jones, S. Tang, B. Zhou, A Cyber Security Ontology for BPMN-Security Extensions, in: 15th Int. Conf. on Computer and Information Technology, IEEE, 2015.

[26] C.L. Maines, B. Zhou, S. Tang, Q. Shi, Adding a Third Dimension to BPMN as a Means of Representing Cyber Security Requirements, in: 9th Int. Conf. on Developments in ESystems Eng., 2016.

[27] M.E. Chergui, S.M. Benslimane, A Valid BPMN Extension for Supporting Security Requirements Based on Cyber Security Ontology, in: 8th Int. Conf. on Model and Data Eng., Springer, 2018.

[28] A. Rodríguez, E. Fernández-Medina, M. Piattini, A BPMN Extension for the Modeling of Security Requirements in Business Processes, Trans. Inf. Syst. (IEICE) 90-D (4) (2007).

[29] K.S. Sang, B. Zhou, BPMN Security Extensions for Healthcare Process, in: 15th Int. Conf. on Computer and Information Technology, IEEE, 2015.

[30] I. Essefi, H.B. Rahmouni, M.F. Ladeb, Integrated privacy decision in BPMN clinical care pathways models using DMN, Procedia Comput. Sci. 196 (2022) 509–516.

[31] E. Bazhenova, F. Zerbato, B. Oliboni, M. Weske, From BPMN process models to DMN decision models, Inf. Syst. 83 (2019) 69–88.

[32] Y. Cherdantseva, J. Hilton, A reference model of information assurance & security, in: 2013 International Conference on Availability, Reliability and Security, IEEE, 2013, pp. 546–555.

[33] G. Stoneburner, A. Goguen, A. Feringa, et al., Risk management guide for information technology systems, Nist Spec. Publ. 800 (30) (2002) 800–830.

[34] M. Robol, M. Salnitri, P. Giorgini, Toward GDPR-Compliant Socio-Technical Systems: Modeling Language and Reasoning Framework, in: 10th Conf. on Pract. of Ent. Mod., Springer, 2017.

[35] J. Tom, E. Sing, R. Matulevicius, Conceptual Representation of the GDPR: Model and Application Directions, in: 17th Int. Conf. on Perspectives in Business Informatics Research, Springer, 2018.

[36] M. Palmirani, G. Governatori, Modelling Legal Knowledge for GDPR Compliance Checking, in: the Thirty-First Annual Conf. on Legal Knowledge and Information Systems, IOS Press, 2018.

[37] M. Palmirani, M. Martoni, A. Rossi, C. Bartolini, L. Robaldo, Pronto: Privacy ontology for legal reasoning, in: International Conference on Electronic Government and the Information Systems Perspective, Springer, 2018, pp. 139–152.

[38] G. Governatori, The Regorous approach to process compliance, in: 19th Int. Enterprise Distributed Object Computing Workshop, EDOC'15, IEEE, 2015.

[39] M. Rhahla, S. Allegue, T. Abdellatif, A Framework for GDPR Compliance in Big Data Systems, in: 14th Int. Conf. on Risks and Security of Internet and Systems, Springer, 2019.

[40] M. Rhahla, S. Allegue, T. Abdellatif, Guidelines for GDPR compliance in Big Data systems, J. Inf. Secur. Appl. 61 (2021) 102896.

[41] M. Bakhtina, R. Matulevičius, M. Seeba, Tool-supported method for privacy analysis of a business process model, J. Inf. Secur. Appl. 76 (2023) 103525.

[42] M. Barati, O. Rana, Design and Verification of Privacy Patterns for Business Process Models, Blockchain Technol. Innov. Bus. Process. (2021).

[43] Y. Sun, P.B. Kantor, Cross-evaluation: A new model for information system evaluation, J. Assoc. Inf. Sci. Technol. 57 (5) (2006) 614–628.

[44] K. Finstad, The usability metric for user experience, Interact. Comput. 22 (5) (2010) 323–327.

[45] A. Casciani, M.L. Bernardi, M. Cimitile, A. Marrella, Conversational Systems for AI-Augmented Business Process Management, in: Research Challenges in Information Science, Springer, 2024, pp. 183–200.

[46] M. Bernardi, A. Casciani, M. Cimitile, A. Marrella, Conversing with business process-aware large language models: the BPLLM framework, J. Intell. Inf. Syst. 62 (2024) 1607–1629.

[47] L. Pufahl, F. Zerbato, B. Weber, I. Weber, BPMN in healthcare: Challenges and best practices, Inf. Syst. 107 (2022) 102013.

[48] S. Remy, Incorporating organizational aspects into fragment-based case management., in: ZEUS, 2020, pp. 10–17.