A BPM methodology for Artificial Intelligence Compliance

Ilaria Angela Amantea[1,*], Guido Governatori[2,3], Marinella Quaranta[1,4], Marianna Molinari[1,4] and Immaculate Motsi-Omoijiade[3]

[1]Computer Science Department, University of Turin
[2]College of Information and Communication Technology, Central Queensland University
[3]Artificial Intelligence and Cyber Futures Institute, Charles Sturt University
[4]LaST-JD, Univeristy of Bologna

Abstract

The Artificial Intelligence Act (AI Act) is a regulation that is changing the adoption of AI systems in European Union. It sets requirements for AI systems to be used in European Union, and AI systems that do not abide by those provisions are subject to fines or excluded from the EU market. We present a theoretical methodology for the compliance of AI systems based on Business Process Management (BPM) techniques. The proposed methodology is twofold: it presents how to apply BPM to processes involving AI systems, and it introduces the BPM methods needed to develop an AI system that complies with the AI Act. In this paper, we use a medical case study to show how to apply every single step of the explained methodology even if the methodology is not field-specific. In fact, the Artificial Intelligence Methodology (AIM) is designed to be generic and suitable to be applied whenever developing and using any AI system to improve a business process or even just to perform a single component/task of the process itself.

1. Introduction

The use of Artificial Intelligence (AI) devices in almost every field has become both ubiquitous and inevitable. The recent AI Act[1] establishes guidelines for the use of AI in different fields and mandates certification of compliance to enter the EU Market. The AI Act is purposely structured to regulate the use of AI systems, describing requirements, limits, and obligations. It does not specifically refer to a single AI, but it takes a risk-based approach to AI regulation, providing a scale of risk related to the use of AI in a specific field. The higher the risk, the stricter the rules, which means that the more an AI system has the potential or the capacity to cause harm to society, the more requirements it will have to comply with.

However, similar to prior European legislation, it has a wide scope and a general approach. To specify some aspects of the prescribed provisions, the EU publishes other soft laws and frameworks, including general guidelines, recommendations, best practices, and others. For example, the Medical Device Regulation was established as the main framework for medical devices in the EU, and, to make its scope clearer, the Guidance on Qualification and Classification of Medical Software complemented it.

However, like all European legislation, the Act lays down general guidelines without providing rules. While this leaves scope for the Member States to tailor provisions to their unique national contexts, it further extends the time it takes for legislative clarity and uniformity. This time frame is further extended by the AI Act's scope, which would apply to every IT system in which there are even just a few automatic tasks involving every level of risk. Therefore, in less than two years, it will be necessary

PLC - Processes, Laws and Compliance workshop, in conjunction with ICPM 2024, October 14, 2024, Lyngby, Denmark
*Corresponding author.
ilariaangela.amantea@unito.it (I. A. Amantea); g.governatori@cqu.edu.au (G. Governatori); marinella.quaranta@unito.it (M. Quaranta); marianna.molinari@unito.it (M. Molinari); imotsi@csu.edu.au (I. Motsi-Omoijiade)
0000-0003-1329-1858 (I. A. Amantea); 0000-0002-9878-2762 (G. Governatori); 0000-0003-2691-0611 (M. Quaranta); 0009-0003-1832-8135 (M. Molinari); 0000-0003-1650-701X (I. Motsi-Omoijiade)

[1]Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act).

to put in place systems that ensure compliance despite the continuing generic nature of the guidelines to achieve compliance. Therefore, the main question is:

How can compliance of an IT system with the AI Act be verified?

One of the issues we have to address is that AI systems typically deal with large volumes of data, and typically the amount of data and parameters surpass what humans can deal with. Thus, it has been argued that only AI systems can check an AI system. The contribution of this paper is to provide a methodology able to address this necessity. In particular, our methodology will answer to the following questions:

- How can a Business Process Management (BPM) system comply with the AI Act using an AI system?
- How can BPM methodology be used in an AI system given that a) an AI system is not based on a typical workflow system and b) an AI system is best capable of checking the large volumes of data used by an AI system?

With these questions in mind, this paper is structured in 3 sections. Firstly, a legal background of the AI Act and of how it relates to Business Process Management sector will be provided. This will be followed by the presentation of our *Artificial Intelligence Methodology (AIM)* and for each point we provide an example of possible application in business processes within the health sector. The final section of the paper will provide authors' remarks, conclusions and perspectives for future works.

2. Background

2.1. Legal background and AI Act

To understand the logic of the AI Act intervention, it is necessary to focus on the European legal background it is connected to. First, the Data Governance Act and the Data Act, as they deal with removing restrictions on the free circulation of data, to facilitate access and use. Second, the Digital Market Act and the Digital Services Act, which are, instead, regulatory interventions that subject platforms to substantial and procedural requirements that must safeguard the functioning of the market and protect the interests of third parties. Last, but not least, the General Data Protection Regulation (GDPR), which aims to ensure that data circulation occurs in compliance with fundamental rights.

The balancing of different interests and principles embedded in these disparate legal provisions has been an ongoing consideration in the development of the AI Act. Analyzing legal sources and their intersection is fundamental for understanding the trade-offs that have occurred. No legislation explicitly balances each factor in advance, thus it is important to analyze the intersection between the already in-force legislation and the AI Act [1].

Nonetheless, the AI Act represents the first regulatory document exclusively dedicated to this discipline.

2.1.1. Structure of the proposed AI regulation.

The regulatory model of the EU conformity mark procedure, already used to regulate the circulation of products, is followed. Therefore, there is a uniform legal framework and a structure that provides a risk-based approach. In fact, obligations are established for suppliers of artificial intelligence tools sized according to the level of risk that AI may entail. There are 4 possible categories of AI tools, with as many regulatory tools corresponding to the different intensity of the risk:

- **Unacceptable risk**. AI tools that can harm vulnerable people or provide social ranking are made objects of an absolute regime. In other words, the use of this kind of AI tool is prohibited, including anything that constitutes a clear threat to people's rights.

- **High risk**. In order to be authorized to place on the market, producers belonging to this risk category must: adopt systems designed to mitigate risks; guarantee the quality of the data that feed the systems; provide clear and appropriate information for the user; guarantee forms of human surveillance; as well as high levels of robustness, safety and precision.
- **Limited risk**. At this level, the regulation only prescribes transparency obligations, such as ensuring that natural persons are informed that they are interacting with an AI system.
- **Minimal risk**. At this level, the regulation does not include specific obligations, unless the right of companies to adopt additional codes of conduct, to be respected on a voluntary basis.

2.2. BPM and AI Act

Each business is based on processes aiming to optimize them to improve quality, increase revenue, manage process changes, and reduce costs and time [2, 3, 4]. To achieve this maximization, more and more companies are increasingly turning to new technologies and, in recent times, to AI.

The business process analysis aims to define and engineer a model to be verified and validated by system experts. One of the main outputs is the creation of visual models of processes (i.e., process maps or flowcharts). These diagrams depict the sequence of activities and various crossroads (gateways), which lead to different routes depending on the choices made. A business process model is a self-contained, temporal, and logical order in which a set of activities are expected to be executed to achieve a business goal. Typically a process model describes what needs to be done and when (control flow), who is going to do what (resources), and on what it is working on (data). In this context, a possible execution, called process trace or simply trace, is a sequence of tasks and events respecting the order given by the connectors.

In this perspective, a key topic of interest for BPM concerns the management of compliance, i.e. the analysis of compliance of the process with the norms [5, 6]. The necessity of satisfying regulations or laws forces organizations to redesign their internal processes, in the context of change management [7]. The increasing pressure from regulatory authorities on organizations led to the development and application of Compliance Management Frameworks (CMFs). In this context, compliance management can be addressed at the operational level by focusing on business processes, intended as the set of activities accomplishing a specific organizational goal [8].

According to this reasoning, a business in a high-risk field that wants to improve itself by introducing even just one automatic task with the use of AI has to be compliant with not only all previous legislation already related to the field of the business but also with the AI Act.

The main problem is that, the AI Act mandates generic conditions for AI systems and delegates the establishment of requirements to domain-specific regulations. However, currently, such domain-specific regulations do not exist. In fact, as all EU Regulations, first, the Regulation is issued stateing the general objectives, and then, the detailed regulations are issued by the European Union itself and by the member states, which establish the detailed rules for step by step application. Therefore, even after the entry into force of the act, as an act of the European Union, it will contain objectives without providing detailed guidelines on their achievement. We will need future Member State regulations to know the details. This means that we will still be facing a long period void of normative details.

There are some methodologies for the compliance of the AI Act, such as [9]. However, they are purely theoretical or consider only the topic of compliance, not considering the integration of compliance in business processes. Considering compliance and business processes separately does not always guarantee the efficiency and optimization of the companies themselves in real cases [10].

The goal of this paper is to provide an example of a healthcare process that wants to be improved with an AI and the regulatory provisions that that process will need to be compliant with in order to be compliant with the AI Act, introducing a methodology that can be followed to conduct an AI Act-compliant process in a high-risk sector.

3. The AIM

Given the nascent nature of the AI act, the Artificial Intelligence Methodology (AIM)'s goal is not to follow its guidelines, but rather to provide a methodology that can guide AI legal compliance, establishing the most important points to keep an AI compliant and optimize a business process with an AI in a compliant way. This will make it possible to improve business processes with an AI, allowing the business to be competitive and stay in the market whilst staying compliant. This methodology specifically targets companies where automatic activities are carried out during the interim phase before detailed guidelines are enforced.

In particular, the aim of this paper is to show how a BPM system can be compliant with the AI Act, if an AI system is involved in the process; and how BPM methodology can be used to analyze an AI system, even if the AI system is not based on typical workflow.

The three main topics we will focus on are: (1) Type of existing processes, (2) Logs and data, and (3) Compliance and Conformance.

In the next paragraphs, we will analyze each point in turn, and we will provide a subsequent example in the healthcare sector using AI in order to give a practical idea of the methodology application.

3.1. Types of Existing Processes

There are three main situations when we want to analyze a process:

Case 1: A well-defined process. There are complete (and possibly correct) process models, where the structure and the order of the activity is given, and where each single activity is well-defined. It can be analyzed through just BPM compliance rules.

Case 2: A partially defined semi-automatic process. Some part of the process is defined but not all. For example, the high-level process or some sub-processes are well-defined but the whole process is not defined or can be defined at the same detailed level.

Furthermore, if logs are available, process mining techniques can be helpful to statistically extract some passages not defined to recreate the whole process and to make the validation of the process itself.

An example of these kinds of processes is healthcare process in which there are a lot of detailed guidelines for each procedure. In this example, the big process involving the whole hospital generally cannot be defined in every step, as different medical situations might have different reorganization needs, based on specific times and specific situations.

If the logs are available, and missing passages are somehow automatically recognisable, meaning that they are already recorded by logs or can be traceable and reconstructed with some manual features (similar to, for example, Credit Scoring systems). However, if there are some automatic tasks and some decisions are taken based on the output of an automatic activity, this process should be subject to the rules of the AI Act for high-risk systems, as there is a significant impact on citizens.

In sum, in both case 1 and case 2 the process are well or almost well-structured and defined. Therefore, we can say they are explainable. AI systems with these kinds of processes would be compliant with the AI Act as they would provide process transparency and outcome transparency. Nonetheless, they will likely be classified as "High-Risk" as they will affect European citizens in several fields.

Case 3: An undefined process. This type of process is based on black box mechanisms, as it does not automatically generate logs. If there is information related to specific parts of the process, e.g. nodes, those specific parts can be analyzed through process mining methods. These methods however can only result in a stochastic definition of the process. If the process involves black box mechanisms and it produces no logs or it avails no logs, there can be no conformity analysis

of the process. In this scenario, the AI system would not abide by the requirements set by the AI Act. However, if only a few steps of the process are available, that is to say if some logs are available, process mining techniques can be used to stochastically define the process. Process mining can be used to whiten the black box path to reveal the complete structure of the process. This scenario would clear the way for conformity checks and, therefore making it more likely to also comply with transparency requirements of the AI Act.

3.2. An Healthcare Process using AI

As has been previously mentioned, in order to demonstrate our methodology and its application, we will use a healthcare process as an example.

In the healthcare field, it is common to find a defined high-level process and well-detailed sub-processes related to specific and technical situations, but not well-defined processes in middle-level operations.

We start with a basic use of AI in healthcare: an algorithm to help in scheduling patients. The scheduling of the patients is typically made by hand, by a doctor, or an administrative staff member, based on some criteria depending on the type of list under consideration.

The process we will consider in this paper is based on a real process of scheduling appointments of patients on a waiting list of the interventional radiology. The traditional scheduling is made by two doctors, who are the radiologists that will make the surgical intervention. Thus, each of them schedules their patients, according to their availability, their professionalism, the availability of the resources (human and material) needed, and, the most important, according to a wide range of medical information related to the patient's specific illness and their general clinical situation. This involves, for example, taking into consideration the fact that some treatments need patient preparation, that takes a specific amount of time (like fasting, or one or more medicines a day or a week before the treatment). Additionally, in the case of specific pathologies, there are specific time-frames cannot be exceeded (e.g., after the hip rupture you need to intervene within 72 hours to avoid side effects). Furthermore, in most instances, the family doctor or the doctor of a specific hospital department writes the so-called "Clinical Question" note, specifying the patient's situation, why in his/her opinion a surgical intervention is needed, and which kind of surgical intervention is needed. However, after this sequence of actions, it is the radiologist doctor responsible for the intervention and who has to evaluate the situation, including evaluating what type of intervention is needed and whether or not it is possible, which type of procedure has to be done, and what types of risks are involved with that particular patient. Adding further complexity is the fact that in some cases the patient is a pluripathological patient, with a lot of different illness, thus treatment good for one pathology can damage other organs (e.g. the use of general anesthesia in very elderly patients would risk overloading other organs). A final factor to consider is the competence of the doctor where the level of complexity of the procedure or intervention determines the level of expertise, experience and seniority of the doctor required.

3.2.1. The Process

Fig. 1 shows how to create a tool enable the automatic scheduling of patients with the support of an AI algorithm. Here, the goal is to insert patients in different waiting lists, not just following the chronological criteria of the one that arrives first will pass first, but also considering the different data of the clinic dossier of the patient, the medical guidelines, and match other important data like staff and resources available, clinical timing, etc in order to assign a weight of priority to each patient. In this way is possible to obtain waiting lists that are as much as possible optimized at different levels: clinical, logistic, etc.

The process is divided into two main steps:

- *Development*: to set and train an AI algorithm at the beginning, and to allow it to subsequently "auto-optimize" itself every time that new data is introduced or every time that a human corrects/reports an error of the output.

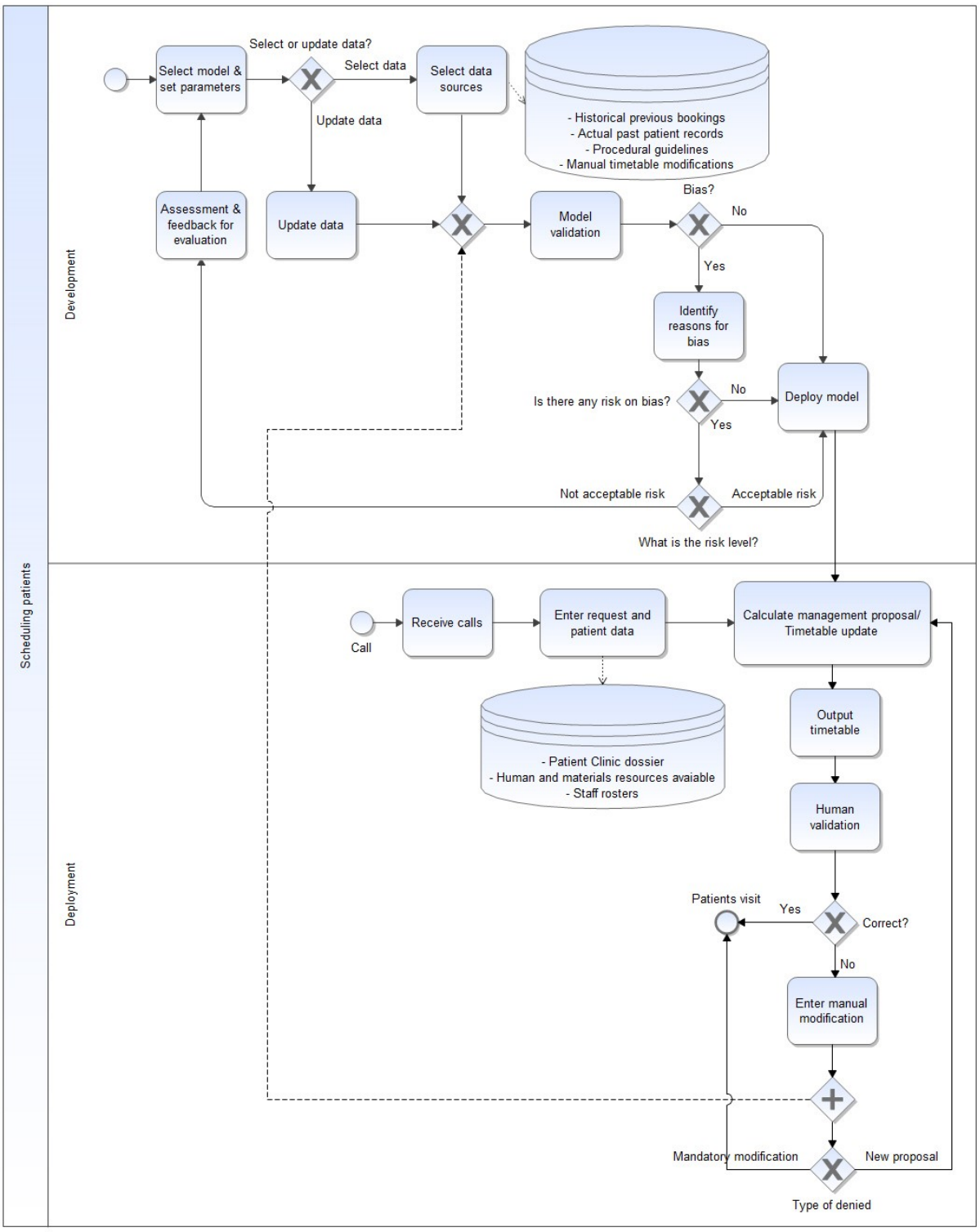

Figure 1: Process of patient's scheduling with AI.

- *Deployment*: that consists of the real activities of the scheduling.

Development. Once the AI model is selected and the parameters are settled, it is important to define the data sources from which the AI algorithm gets trained and updated. In our case, the data sources can be historical previous bookings, the actual past patient records, the manual timetable modifications (from the merging of these three elements, it could be possible to learn from the past organization, based on real cases, real pathologies and possible modifications), and the procedural medical guidelines

(to understand the legal obligations, medical obligations, and the constraints).

The model has to be validated. If there are no biases found, the model can be deployed. If some biases are found, it is important to identify the causes and evaluate each one of them in relation to the level and type of risks. If the risks are acceptable, the model can be deployed, in other cases a reassessment of the model is needed along with the setting of a new model or new/updated parameters.

Deployment. In the traditional patient booking process, the starting point is the call for a new patient booking request and the entering of his/her personal data. With this model, once a new patient arrives and the model is deployed, the AI algorithm can calculate or manage a timetable scheduling patient proposal.

To calculate the correct timetable, so the correct position of the patient, or the priority of this patient among the others in the list, the model takes into account the patient's clinical dossier (so the clinical history of the patient, including the personal data like age, gender, living place that can affect the diagnosis), human and material resources available (for example if there is a specific specialized doctor this day at that time, if some consumable materials are available, if is not already booked a specific machine to the exam), and the staff rosters (for example taking into account vacations, festivity, temporary sickness of the medical staff).

Once the output is given, a human can make a verification check. If the proposed scheduling is acceptable it is possible to proceed to the confirmation of the booking and the patient's visit.

In case the proposed timetable is not correct the human can modify the booking. In this case, two main paths occur:

- On the one side, this manual modification will become part of the training of the model becoming a correction of the future upgraded outputs.
- On the other side, in the specific case, if the manual modification is mandatory the patient is booked/visited as stated from the manual corrected timetable. If the modification is not mandatory, the algorithm can propose a new updated model. In fact, in this case, the manual modification is already part of the sources taken into account from the AI (point above).

3.3. Log and Data

Even if the map of the process (for example, using process mining techniques on the AI system log) is not available, the process can be mapped by the use of logs. Also, the logs can be used to validate the process map.

Process mining is a technique already widely used for this purpose, even in the medical field [11, 12, 13].

There are two main problems with using the logs for the automatic creation of the real process. The first is the availability of data (if the business collected them, if it is possible to collect them, if the database is in electronic format and not on paper). The second is whether the log database has all the technical and legal characteristics required.

About the second point, it is important to observe that the AI Act has prescribed some characteristics related to databases, in particular to logs of AI systems and their preservation:

- According to Art.10, information about databases must be available, including information about data collection, the origin of data, the original purpose of collection, preparation processing operations, formulation of assumptions, availability, quantity, and suitability of data. Also, it prescribes the examination of biases, providing for detection, mitigation, and prevention measures. Additionally, data gaps and shortcomings must be identified together with related controlling measures.
- According to Art. 15, AI systems must bear robustness and cybersecurity, and need to be resilient to errors through technical redundancy solutions (backup and fail-safe plans). As for "external robustness" AI shall be built with mitigation measures reducing possible biased outputs that

affect latter inputs ("feedback loops"). As for cybersecurity, the AI system shall be built to be resilient against attempts to alter AI use by preventing detecting responding measures to resolve and control hacking attacks aiming at data poisoning, model poisoning, or adversarial modeling.
- The most relevant AI Act Article related to logs is Art.12. It prescribes the technical capacity of automatic recording events ('logs') throughout the lifetime of the system, they involve the capabilities of recording from the start date and time to the end date and time of each use, the reference database against which input data has been checked by the system, the input data for which the search has led to a match, and the identification of the natural persons involved in the verification of the results. Finally, it also prescribes for the identification of situations that may result in the AI system presenting certain kinds of risks[2].

The AI Act prescribes logging capabilities for databases, however, the technical implementation of such capabilities is not described and other EU and national documents will likely establish more precise and clear standards. Until this is specified, our methodology aims to create a compliance path for businesses that currently are interested in entering their medical AI system in the EU market.

It is important to focus attention on the fact that the main characteristics for the logs and dataset required by the AI Act are almost the same required for process mining. A slight difference is that, typically, in process mining for business processes, the logs are transactional. For AI systems they record events and the operations on data; however, for the purposes of identifying their behaviour, we can consider their logs as transactional, and apply existing process mining techniques.

3.4. An Healthcare Log

We will follow the previously established example of patients scheduled for surgery in Interventional Radiology. This example is extracted from a real day in the Interventional Radiology department of an Italian hospital.

On average there are from 6 to 10 patients each day.

Once the patient appears on the list of the surgery, he/she has to be scheduled for the surgery for the present day or within 3 or 4 days maximum. In some instances, medical emergencies require patients to be scheduled within 1 or 2 hours maximum, and in other situations patients have to be scheduled after 3-4 days and not before for various medical reasons (e.g. because medical preparations are needed or because the effect of a drug will start or stop after some defined time).

Finally, there are some criteria for the creation of the sequence of the patients within the day. The first to pass are the patients who have to undergo the so-called "clean procedures", then those subjected to "dirty procedures", and finally patients who are infected or contaminated (e.g. Covid-19 patients).

Table 1 shows a portion of a real log of scheduled patients who need surgery in Interventional Radiology on a specific day.

In particular, the log reports the sequence of the progressive number of patients in the day (*C*), the identification number of each patients (*ID*), the number of the Medical Dossier (*Med Dos*), the reason why the patients need the surgery according to the doctor that sent the patients to the surgery room (*Clinical Question*), the type of surgery procedure made (*Procedure*) and their typology if clean (*C*) or dirty (*D*), the booked day and hour for the surgery (*Booked for*) and the real-time of the patient arriving to the end of the surgery (*Timestamp*).

Each day some different situations can happen that can change the established scheduling. For example, on the 19th of September 2022, patient number 1-3-4-5 was booked. When the working day began, patient number 1 was canceled. In the meanwhile, probably one of the hospital departments did call the surgery department as they discovered that a new patient needed urgent surgery (so the same day). They called to understand if and when it would be possible to insert the patient. Given the cancellation of the first patient and then the slot freed, there has been given immediate availability to receive it. This explains why the strange time of booking (07:52), as probably the booking was made "for immediate need" and the patient did arrive at 08:15, which was the time of patient transportation.

[2]Article 65(1) of the AI Act.

Table 1
Log of patients data and surgical scheduling timetable of a day.

C	ID	Med Dos	Clinical Questions	Procedure (C)-(D)	Booked for	Time
1	1146346	M1146346	TACE with EMBOCEPT on HCC infiltrating in S8	69-99252 - Local regional chemioembolization (C) 69-8847 - Arteriography tripod celiac desiase (C) 69-88495 - Hepatic arteriography (C)	19/09/22 08:00	Canc
2	1374028	M1374028	MonoJ bilateral replacement in Bricker	69-39993 - Extravascular Interventional Control (D)	19/09/22 07:52	8:15 8:54
3	2268135	M2268135	Left pyelotomy placement in patient with anastomotic stenosis after cystectomy+ orthotic neobladder	69-55121 - Percutaneous monolateral pyelostomy (D)	19/09/22 09:00	09:00 10:07
4	4408398	M4408398	Patient known to you, recent fastostomy replacement. Requires revision for partial leakage of the fastostomic probe	69-4311 - Percutaneous gastrostomy (D) 69-39993 - Extravascular Interventional Control (D)	19/09/22 11:00	11:00 12:15
5	0265286	M0265286	Control in patient undergoing hepatic resection and packaging of hepatic fasting anastomosis carrying transanastomotic bile drainage Contact isolation for KPC	69-87541 - Control Cholangiography (D)	19/09/22 13:00	13:00 13:25

3.5. Compliance and Conformance

Compliance[3] is the set of measures in place in an organisation to ensure the (business) activities satisfy the (legal) requirements they are subject to [15, 14].

As we discussed the AI Act covers sectors where the use of IT systems with some degree of autonomy is deemed as risky. Here we propose to use an (automated) IT system to determine if another IT system complies with the AI Act. To do this, we need two components: (1) a set of formal specifications of the legal requirements and (2) a set of specifications describing the behaviour of the IT system. For (1) we selected Defeasible Deontic Logic (DDL) [16]. DDL provides a conceptually sound and computationally efficient representation of normative specifications, and it has been successfully applied in many domains. Unlike other techniques, such as NLP which proceeds in an automatic manner and only on a semantic basis, the logical representation in DDL is not done automatically but manually by legal experts. This allows not only the literal interpretation to be considered during formalization but, also that all other types of interpretations that a legal expert must consider when interpreting a law are not misled.

For (2) we propose to represent the behaviour of an IT system as a business process model (or a set of business process models). The proposed combination of (1) and (2) allows us to adopt the Business Process Compliance (BPC) methodology [17] to verify that the IT system complies with the AI Act (and the related secondary legislation).

The first step of the methodology is to formalise the norms. In DDL, a norm is represented as an IF… THEN$\cdots$ rule, where the IF part describes the conditions of applicability of the rule/norm and the THEN part is the legal effect of the norm. There are two types of effects: a rule defines a term in the context of the set or norms (*constitutive rule*), or the rule mandates that a normative requirement –obligation, prohibition, permission–is in force if the conditions of applicability hold (*normative rule*). Thus, we have expressions of the form

$$r\colon a_1, \ldots, a_n \Rightarrow_X c$$

[3]As pointed out in [14] the terms compliance and conformance have been used with slightly different meanings in the Business Process community, and they are effectively synonyms in the day-day parlance and in the legal domain.

where r is the rule label, unique for each rule; $a_1, \ldots, a_n$ are the conditions of the applicability (represented as propositions or deontic propositions); c, again a proposition, is the conclusion or effect of the rule; and X specifies the type of rule. If $X = C$ we have a constitutive rule, and the effect is simply c; otherwise, we have a normative rule, and the conclusion c is in the scope of a deontic operator. The operator depends of the value of X, where we have the obligation or prohibition of c, if $X = O$ or that c is permitted if $X = P$. The language and the reasoning mechanism of DDL allow us to deal with a complete family of legal requirements [18], including violations and compensatory measures, and a rich and natural treatment of exceptions [16].

The second component is to have a business process model corresponding to the behaviour of the IT system. At the end, for the BPC methodology, a process is described by its set of traces, where a trace is a (finite) sequence of tasks, e.g., $T = \langle t_1, t_2, \ldots, t_n \rangle$. It is important to notice that regulatory compliance is not limited to the activities (tasks) done and the order in which they have been executed but, in most cases, requires examining what has been achieved or done by the task, what and how data has been used. Accordingly, we need to know what the effects of the tasks are. To achieve this, we have to enrich the description of the process with annotations, where each task is associated with a set of propositions. These propositions describe what is known to hold after a task. Based on the annotations, we can have a function $State$ that, given a trace T and a natural number n, returns the state of the process (trace) after executing the n-th task in the trace.

The procedure to check whether a business process complies with a set of norms consists of the following steps:

1. Select a trace, T, traverse it, and for every task t_i compute $State(T, i)$.
2. Use $State(T, i)$ as input of the set of rules to determine the set of legal requirements (obligations, prohibitions, permissions) in force based on the state of the trace (including the requirements pending from the previous state);
3. Check whether the obligations and prohibitions have been satisfied, violated, or are pending.

A trace is *compliant* if at the end of it, there are no violations, or all violations have been compensated (*weakly compliant*, and there are no pending obligations. A process is compliant if all traces are compliant.

The AI Act mandates that AI systems be certified of compliance (both for development and deployment) and that they must monitor execution to ensure they obey the relevant norms (e.g. Article 17). Notice that AIM can address both aspects.

It should be clear that for the application of AIM, we need to have process models for the IT system and the relevant annotations. In Section 3.1, we described three types of process. AIM depends on the integration of BPC and Process Mining. For what we call well-defined processes, process mining can be used to populate the annotations to verify compliance when the system is designed (and tested) before deployment and to extract the precise task data to be used to monitor whether the execution of an instance complies with the norms.

For partially defined processes, Process Mining, in addition to what it can do for well-defined processes, can be used to fill the gap to provide more complete information about the structure of the process. Finally, for the last type of process, Process Mining is used to extract putative processes describing or approximating the (expected) behaviour of the AI system. Furthermore, it can detect if the behaviour is drifting or deviating from the behaviour previously established as the expected behaviour. According to AI Act, when there are changes in the behaviour of and AI system, the system needs a certification of compliance.

3.6. Is the Process Compliant?

Following our example, having the process explained in Fig. 1, it is important to understand if the process is compliant with the law. As previously mentioned, there are a lot of laws and regulations involved in a process, with even more legal and regulatory obligations required of healthcare processes.

The AI Act specifies the use of AI and logs as the most recent addition to prior regulations, laws, and guidelines at different levels. The process analyzed is a process using AI that is able to balance some parameters and propose a correct scheduling of patients for Radiology Interventional surgery.

To illustrate how compliance detection occurs, we will take into account an article of the AI Act, and a procedural rule about surgery. The article of the AI Act gives indications for the development of the AI system. It relates to the creation and maintenance of the first dataset (dataset presented in Fig. 1, lane *Developement*).

The procedural rules about parameters to take into account about a specific surgery are fundamental, and that is part of the second dataset (dataset presented in Fig. 1, lane *Deployment*). Which means, that this rule is one of the parameters (therefore of the logs) to be considered in the specific scheduling of the specific patient (thus, in case the patients present that type of illness).

Article 10 of AI Act The most relevant article in the AI Act for compliance and conformance purposes is Article 10 "Data and Data Governance", which sets out a number of general requirements to build an adequate dataset.

In particular, as an example of DDL formalization of the Art. 10, we chose paragraph 2 letters a), aa) and c). The article recites

> Training, validation and testing data sets shall be subject to appropriate data governance and management practices appropriate for the intended purpose of the AI system. Those practices shall concern in particular,
> (a) the relevant design choices;
> (aa) data collection processes and origin of data, and in the case of personal data, the original purpose of data collection
> (c) relevant data preparation processing operations, such as annotation, labelling, cleaning, updating, enrichment and aggregation.

The above provisions are formalised as follows

$$a\colon AISystem, HighRisk \Rightarrow_O DescribeDesignChoices$$
$$aa\colon AISystem, HighRisk \Rightarrow_O DataCollectionProcess\&DataSource$$
$$aa.1\colon AISystem, HighRisk, PersonalData \Rightarrow_O PurposeDataCollection$$
$$c\colon AISystem, HighRisk \Rightarrow_O DataPreparationOpeations$$
$$c.1\colon Annotation, Labelling, Cleaning, Updating, Enrichment, Aggregation \Rightarrow_C DataPreparationOpeations$$

Procedural Surgical Rule. For an AI medical system, specific features related to its medical purpose lead to specific compliance and conformance checks. These checks are established by other specific medical guidelines.

We selected as a relevant medical guideline: the Multi-company Italian Recommendations for the integrated clinical management of patients with hepatocarcinoma. As an example, we selected one guideline related to the solid focal lesion which states:

> In case of detection of a new solid focal lesion <1 cm, a three-months ultrasound surveillance should be activated. If the lesion grows to $\geq$10mm, proceed as per the scheme proposed for these nodules. If the lesion does not grow in the next 2 years, it should return to the six-monthly surveillance.[4]

This medical guideline can be represented by the following rules:

$$r_0\colon SolidFocalLesion, dimension \geq 10mm \Rightarrow_O NoduleScheme$$

[4]See https://sirm.org/wp-content/uploads/2021/04/304-Documento-intersocietario-AISF-AIOM-IT-IHPBA-SIC-SIRM-SITO-2016-HCC-raccomandazioni-multisocietarie.pdf.

$$r_1 : NewSolidFocalLesion, dimension < 1cm, \Rightarrow_O SurveillanceThreeMonths$$
$$r_2 : SolidFocalLesion, [O]SurveillanceThreeMonths, dimension \geq 10mm$$
$$\Rightarrow_O NoduleScheme$$
$$r_3 : SolidFocalLesion, [O]SurveillanceThreeMonths, \neg growthTwoYears$$
$$\Rightarrow_O SurveillanceSixMonths$$
$$conflict(SurveillanceThreeMonths, SurveillanceSixMonths)$$
$$r_3 > r_1$$

In conclusion, once we have both the process mapped and the rules formalized, the running's traces will be able to detect if the process is compliant or not; and, in this second case, which are the specific activities that are not compliant.

4. Conclusions and Remarks

The use of AI is pervading every industry. In a few months, it will be an integral part of almost every business. This will lead even the most reluctant companies to use it soon in order not remain in the market and to retain competitive advantage.

The AI Act provides stringent regulation providing requirements and obligations on the production and sale of AI at European level covering the entirety of European territory. As the AI Act provides generic guidelines of requirements without specifying the guidelines to meet them, the various member states will have to establish additional provisions, after the enactment of the Act, to produce the detailed regulations.

Meanwhile, companies must be compliant with the AI Act and they will have a maximum of two years (which will take effect not from the enactment of States regulations, but from the enactment of the AI Act). Furthermore, it is plausible to assert that given the huge amount of data required to run an AI system, only an AI system will be able to check another AI system. Therefore, automating compliance of AI systems is one of the current biggest challenges.

The AIM is a methodology that can guide through the strategic points of a business, and of the AI Act requirements, creating a guideline to check the compliance of the AI system in the business that can work as of now. This paper shows a theory of a methodology that will be applied, verified, and tested on real use cases after the official publication of the AI Act.

Acknowledgments

This study was funded in the context of the European Digital Innovation Hub (EDIH) for the Healthcare Digital and AI support and innovation (Circular Health European Digital Innovation Hub - CHEDIH) (www.chedih.eu) in Piedmont Region, Italy.

References

[1] M. Quaranta, I. A. Amantea, M. Grosso, Obligation for ai systems in healthcare: Prepare for trouble and make it double?, The Review of Socionetwork Strategies (2023) 1–21.

[2] W. M. Van der Aalst, J. Nakatumba, A. Rozinat, N. Russell, Business process simulation, in: Handbook on BPM 1, Springer, 2010, pp. 313–338.

[3] W. Abo-Hamad, A. Arisha, Simulation-based framework to improve patient experience in an emergency department, European Journal of Operational Research 224 (2013) 154–166.

[4] A. Di Leva, E. Sulis, A. De Lellis, I. A. Amantea, Business process analysis and change management: The role of material resource planning and discrete-event simulation, in: Exploring Digital Ecosystems, Springer, 2020, pp. 211–221.

[5] M. Dumas, M. La Rosa, J. Mendling, H. Reijers, Fundamentals of business process management, volume 1, 2nd ed., Springer, 2018.
[6] W. M. Van der Aalst, Business process management: a comprehensive survey, ISRN Software Engineering 2013 (2013).
[7] J. Hayes, The theory and practice of change management, Palgrave Macmillan, 2014.
[8] I. A. Amantea, L. Robaldo, E. Sulis, G. Governatori, G. Boella, Business process modelling in healthcare and compliance management: a logical framework, Journal of Applied Logics—IfCoLog Journal of Logics and their Applications 9 (2022).
[9] L. Floridi, M. Holweg, M. Taddeo, J. Amaya, J. Mökander, Y. Wen, Capai-a procedure for conducting conformity assessment of ai systems in line with the eu artificial intelligence act, Available at SSRN 4064091 (2022).
[10] I. A. Amantea, Methods and tools for analysis and management of risks and regulatory compliance in the healthcare sector: the hospital at home–hah (2022).
[11] J. Munoz-Gama, N. Martin, C. Fernandez-Llatas, O. A. Johnson, M. Sepulveda, E. Helm, V. Galvez-Yanjari, M. Comuzzi, Process mining for healthcare: Characteristics and challenges (2022).
[12] M. Di Cunzolo, A. Guastalla, R. Aringhieri, E. Sulis, I. A. Amantea, M. Ronzani, C. Di Francescomarino, C. Ghidini, P. Fonio, M. Grosso, Combining process mining and optimization: A scheduling application in healthcare, in: BPM 2022, Springer, 2022, pp. 197–209.
[13] I. A. Amantea, E. Sulis, G. Boella, R. Marinello, D. Bianca, E. Brunetti, M. Bo, C. Fernandez-Llatas, et al., A process mining application for the analysis of hospital-at-home admissions, Studies in health technology and informatics 270 (2020) 522–526.
[14] H. Groesfema, N. van Beest, G. Governatori, On the use of the conformance and compliance keywords during verification of business processes, in: BPM Forum 2022, volume 458 of *LNBPI*, Springer, 2022, pp. 21–37.
[15] M. Hashmi, G. Governatori, H.-P. Lam, M. T. Wynn, Are we done with business process compliance: State-of-the-art and challenges ahead, Knowledge and Information Systems 57 (2018) 79–133.
[16] G. Governatori, A. Rotolo, G. Sartor, Logic and the law: Philosophical foundations, deontics, and defeasible reasoning, in: D. M. Gabbay, J. Horty, X. Parent, R. van der Meyden, L. van der Torre (Eds.), Handbook of Deontic Logic and Normative Reasoning, volume 2, College Publications, London, 2021, pp. 655–760.
[17] G. Governatori, The Regorous approach to process compliance, in: 2015 IEEE 19th International Enterprise Distributed Object Computing Workshop, IEEE Press, 2015, pp. 33–40.
[18] M. Hashmi, G. Governatori, M. T. Wynn, Normative requirements for regulatory compliance: An abstract formal framework, Information Systems Frontiers 18 (2016) 429–455.