[MKM+19] J. Michael, A. Koschmider, F. Mannhardt, N. Baracaldo, B. Rumpe:
User-Centered and Privacy-Driven Process Mining System Design for IoT.
In: Proceedings of CAiSE Forum 2019: Information Systems Engineering in Responsible Information Systems, June 2019.
www.se-rwth.de/publications/

User-Centered and Privacy-Driven Process Mining System Design for IoT

Judith Michael[1], Agnes Koschmider[2], Felix Mannhardt[3], Nathalie Baracaldo[4], and Bernhard Rumpe[1]

[1] RWTH Aachen University, Software Engineering, Aachen, Germany
{michael,rumpe}@se-rwth.de, http://www.se-rwth.de
[2] Karlsruhe Institute of Technology, AIFB, Karlsruhe, Germany
agnes.koschmider@kit.edu
[3] SINTEF Digital, Trondheim, Norway
Felix.Mannhardt@sintef.no, http://www.sintef.no
[4] IBM Almaden Research Center, San Jose, USA
baracald@us.ibm.com

Abstract. Process mining uses event data recorded by information systems to reveal the actual execution of business processes in organizations. By doing this, event logs can expose sensitive information that may be attributed back to individuals (e.g., reveal information on the performance of individual employees). Due to GDPR organizations are obliged to consider privacy throughout the complete development process, which also applies to the design of process mining systems. The aim of this paper is to develop a privacy-preserving system design for process mining. The user-centered view on the system design allows to track who does what, when, why, where and how with personal data. The approach is demonstrated on an IoT manufacturing use case.

Keywords: Privacy-by-Design · Process Mining · Event Log · Access Control · Meta-Model · Privacy Preserving System Architecture.

1 Introduction

The General Data Protection Regulation (GDPR) marks a new era in data privacy. GDPR provides a set of data protection principles, individuals' rights and legal obligations to ensure the protection of personal data of EU citizens. Privacy concerns informal self-determination, which means the ability to decide what information about a person goes where [5]. GDPR imposes organizations to consider privacy throughout the complete development process, which also applies for the design of process mining systems. Process mining uses as input event logs files, which originate from all kinds of systems such as ERP or Internet-of-Things (IoT) systems. To design systems compliant with GDPR, eight privacy design patterns have to be considered: minimize, hide, separate, aggregate, inform, control, enforce, and demonstrate [12]. Privacy can be protected, for example, by means of *hide any personal information that is processed*

from plain view or *data subjects should have agency over the processing of their personal information*. These privacy design patterns have been acknowledged as useful in order to integrate them into the development processes [7]. They can be considered as requirements for the design of privacy-preserving process mining systems. Whereas process mining does not directly use or require to use personal information - the focus is often more on improving on the organizational level rather than the personal one - event logs can expose sensitive information that may be attributed back to individual persons. For instance, events may contain sensitive information pertaining to preferences of workers. Also the traces, i.e., sequences of activity executions, reveal information on the performance of individual workers, which can constitute personal information that workers may want to protect. Some research has been done on cross-organizational process mining, in which organizations are reluctant to share information [14] and guidelines from a practical viewpoint in a consulting context have been published [19]. So far, however, there has not been research on privacy preservation in the area of process mining.
To fill this gap, this paper aims to develop a user-centered system design, which captures privacy in process mining. The system design is exemplified in the context of IoT manufacturing working tasks. It supports data owners (e.g., workers) to control privacy concerns for sensitive data by means of privacy polices and to monitor their compliance (i.e., is the data captured unauthorized?). In this way, it allows data owners to determine more accurately who can do what with which data and allows them to see which privacy concerns are foreseen in which steps of process mining. The definition of the user-centered privacy system design for process mining requires to understand privacy checkpoints in process mining and how to ensure a user-centered access control to event logs. For this, we define an IoT use case to which we refer throughout the paper.

The remainder of this paper proceeds as follows. The next section summarizes related works and shows that no privacy-preserving meta-model exists for privacy mining. Section 3 discusses terms used as input to define the user-centered privacy system design and presents our IoT use case. Section 4 defines the the data model and architecture. Section 5 presents a brief application of the privacy system design in the context of process mining. The paper ends with a summary and an outlook on future work.

2 Related Work

To define the privacy-preserving system design we studied related approaches on (1) privacy-preserving data mining, (2) access control, (3) privacy meta-models and (4) privacy in process mining. Privacy-preserving data mining (PPDM) [2] aims at finding the best suitable privacy preserving technique for the data. The large body of literature on PPDM mainly focus on the hide and aggregate privacy challenges, while privacy concerns of the data provider are mainly disregarded [22]. The privacy-preserving meta-model for event logs as presented in this paper is complementary to PPDM like anonymization measures in order

to fulfill compliance with GDPR. With respect to literature on access control, role-based access control (RBAC) and policy-based access control (PBAC) also known as attribute-based access control (ABAC) have been suggested. ABAC grants access to services based on the attributes possessed by a requester. Thus, it replaces the subject (a user) by a set of attributes [21]. PBAC uses digital policies to guide authorization decisions. Such policies can be built with the policy language XACML. In the context of IoT the advantages of ABAC can be exploited: all information within the organization can be accessed in real-time for all types of requests. The system design presented in this paper relies on ABAC and XACML and has been extended for our purpose.
Privacy meta-models can be found in [10, 11, 4]. Feltus et al. [10] present a model-driven approach for privacy management in business ecosystems. Their privacy meta-model focuses on the privacy in the dynamics of businesses and therefore, only resources, roles and activities are considered for privacy preservation. Grace and Surridge [11] present a formal model of user-centered privacy by using labeled transition systems (LTS) for analysis of a service's behaviour against user preferences. This approach focuses only on data and does not include process mining aspects. In [4], Bergeron proposes a UML profile to model privacy protection for web applications during application design. The restrictions of these privacy meta-models makes them not suitable for our purpose. Therefore, we define a proper meta-model for process mining allowing to consider context information related to environment and location, which is necessary in our IoT use case. Related to event log data, a large body of research exist for security-oriented analysis [20]. For instance, the tool of Stocker and Accorsi [20] allows to configure security concerns (i.e., authentication, binding of duty and separation of duties) when generating synthetic event logs. The literature analysis shows that privacy concerns have been scarcely considered for process mining. Only the work of [16] discusses privacy challenges for process mining, however, without providing a solution how to protect user privacy. To the best of our knowledge, this paper suggests the first system design and privacy-preserving meta-model for process mining.

3 Motivation: Background and Use Scenario

Below, we discuss terms related to the context of privacy and process mining and apply them for the use scenario tracking IoT manufacturing working tasks.

Privacy and Process Mining. The GDPR defines personal data as "any information relating to an identified or identifiable natural person" (referred to as *data provider*) [9]. Privacy protection goes further than security and regulates the authorized access to data based on a lawful basis (e.g., may be bases on consent, but based on legal requirements such as auditing) and organizational measures that should build trust between the individual (i.e., data provider), the entity who process and store the data (referred to as *data controller*) and entities who use or bought the data (referred to as *data consumer*). *Process mining* uses event data recorded by information systems to reveal the actual execution

of business processes in organizations. Since most activities in modern organization are supported by technology each process execution leaves behind a digital trace indicating the occurrence and timing of activities in the databases of the company. Process mining takes event logs, records of the sequence of steps, and discovers a de-facto model of the process that can expose performance information, bottlenecks, workarounds, and much more. In this way, events and traces may contain sensitive information pertaining to data provider and being accessible to data controller(s) and data consumer(s). To a certain degree process mining methods already abstract from such privacy related details by deriving a process model that reveals only the observed sequences of activity execution. However, often occurrence frequencies, performance information, and decision rules are discovered in addition to the basic control-flow of the process [18], which may leak additional information from the event log. Furthermore, process mining is often an iterative process in which multiple process models for different subsets of the event log, filtered according to conditions of interest, are discovered and compared [8]. By discovering several process models and slightly varying the filtering condition it is possible to identify workers. Obviously, privacy preservation should be taken into account for process mining.

Use Scenario: Privacy and IoT Manufacturing Tasks. IoT is a domain with a high demand for privacy and security considerations. The large amount of data, that is tracked and analyzed with e.g., learning (AI) software, can originate from internet-enabled machines, working modules labeled with QR-code and workers equipped with wearable such as smart watches, interacting as autonomous agents forming a complex system. In the context of IoT, GDPR relates to privacy compliance of a large number of attributes such as GPS location, working time and salary. From this data, the working practices and performance of workers can be inferred, which may be considered very sensitive information [15].

To understand which privacy concerns may arise in the steps of process mining (i.e., to understand privacy policies between data provider, controller and consumer) we apply the privacy checkpoint diagram proposed by [16] with six stages of data passes for IoT manufacturing working tasks, see Figure 1.

- *Data source:* given our use case, the sources of data are manufacture information systems, the machine working on, wearables like smart watches, sensors measuring humidity or monitoring malfunctions and (mobile) devices tracking location, identify, etc.
- *Data capture:* data from these data sources is captured when devices and systems log tasks, when recognizing the identity or requesting actions. This stage tracks who does what, when and where (e.g., a worker committed a working task with his smart watch on Nov. 28 at 11:28h).
- *Primary use:* the data controller (e.g., manager representing a company) determines the purposes for which and the means by which the captured data is processed. For instance, the captured data can be used for recommending subsequent tasks for workers. In this way, the data controller decides *why* and *how* the personal data should be processed. The privacy concern of the data provider at this stage is to *control* what kind of and how much information

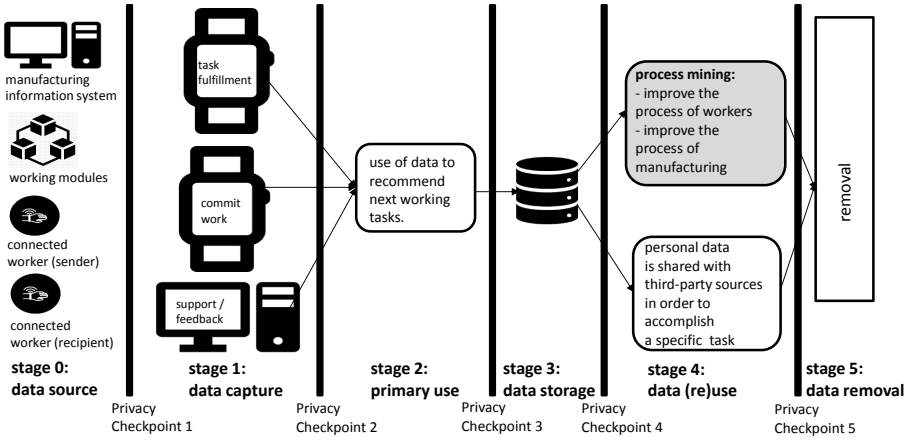

Fig. 1. Identification of data passes and privacy checkpoints for IoT manufacturing working tasks adapted from [16].

other people can obtain from his data [22], while the data controller must ensure an authorized data use.

- *Data storage:* the personal data is stored by the data controller in a database or in event logs.
- *Data (re)use:* at this stage, data from event logs is used for process mining. For instance, the data controller is interested in any compliance violations. Personal data might also be bought by data consumers (e.g., supplier or a quality assurance department, which notifies managers) such as suppliers requiring to demonstrate that the data was retrieved in compliance with GDPR regulations. The duties of the consumer towards the data of providers are specified in a privacy policy and indicate what data is requested and for what purpose and what happens to the personal data once the contract ends.

Although event log analysis becomes relevant at the data (re)use stage, several privacy concerns must be addressed before. Data should not be captured in unauthorized ways (see data capture). Particularly, requirements for event data must be fulfilled in a way that case, timestamp and activity were captured authorized. Also, data should not be processed for unapproved purposes (see primary use), used for unauthorized disposal and violating the policies between data consumers and data controller (see data re(use)). The next section presents a system design supporting these privacy concerns during process mining.

4 User-Centered Privacy-Driven System Design

To ensure user-centered privacy for process mining, the system design relies on privacy policies. First, a context meta-model is introduced, which is used as schema for data storage. Next, the context meta-model is enriched with privacy concepts and process mining concerns captured in a *privacy preserving*

meta-model. Lastly, the architectural model is described allowing to monitor the compliance of policies. First, we introduce the context meta-model.

4.1 Context Meta-Model

Figure 1 shows the *context meta-model*, which is applied for illustration on the use case of IoT manufacturing working tasks. The context meta-model is defined by

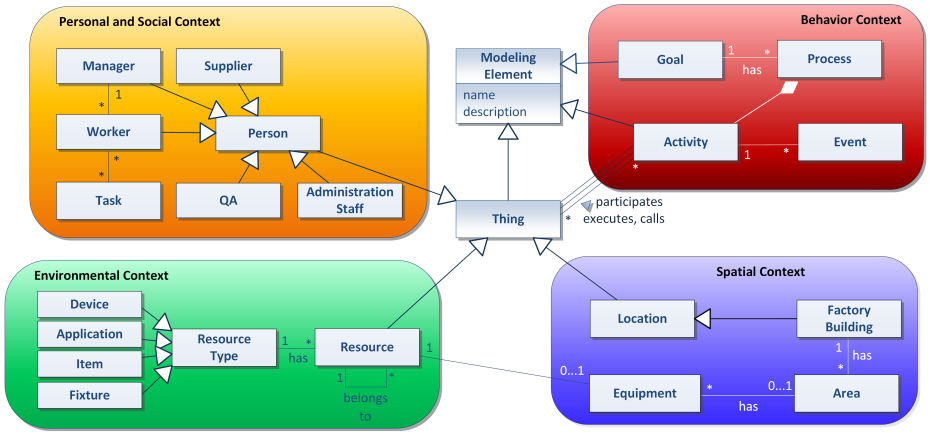

Fig. 2. Context Meta-Model of the Use Case

four contexts. The **Personal and Social Context** describes all relevant *Persons* (e.g., in the use case of IoT manufacturing working tasks: workers, managers, administration staff, suppliers) referring to their abilities, mental and physical information about persons, tasks or duties. The **Behavior Context** addresses the tasks persons do: steps and goals. The Behavior Context consists of an *Activity* and related *Events*. Activities are part of a *Process* with a certain *Goal* including sub-goals. Goals in our use case are e.g., to produce a certain product, to control a production step or to deliver a component. The **Spatial Context** represents all concepts related to venues like *Departments* (i.e., Factory Buildings) that might differ in *Locations*, within *Areas* and certain *Equipment*, which can be placed in these areas. The **Environmental Context** is highly relevant for our use case, as either the usage of certain *Resources* (device, application, item, fixture) by persons is stored as well as the behaviour of these resources by using its sensor data. *Thing* and *Modeling Element* are the meta-concepts. Also, relationships between different contexts can be modeled like activities and events have calling, executing and participating things (either persons, resources or locations). Resources of a certain resource type (device and fixture) can be placed as equipment in an area. Tasks can be related to certain resources. To define restrictions (e.g. a certain activity can only happen in a certain area) the object constraint language (OCL) has been acknowledged as useful. Note that

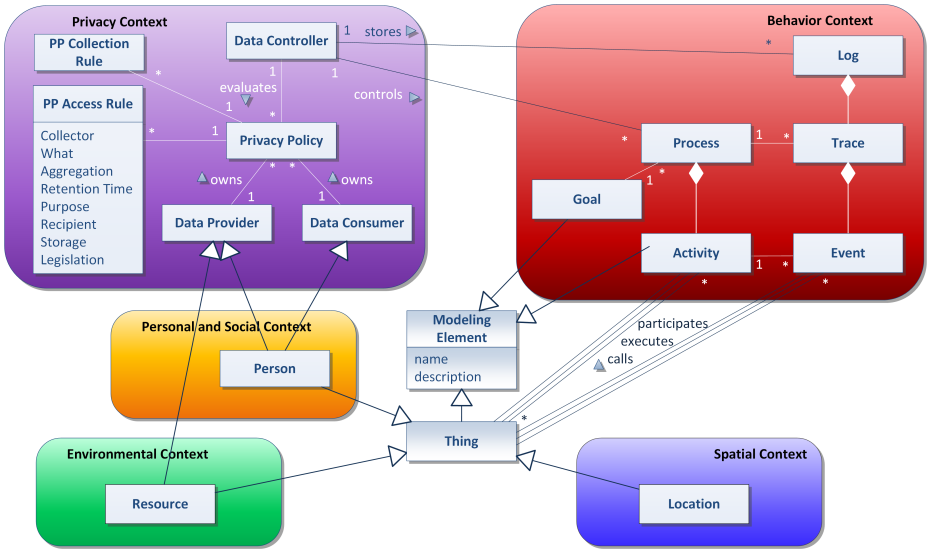

Fig. 3. Privacy Meta-Model for Process Mining

this is only an excerpt of the context meta-model customized for your use case. A complete version of the context meta-model for AAL is described in [17]. Next, we extend the context meta-model with privacy and process mining concepts.

4.2 Privacy Preserving Meta-Model

Fig. 3 shows the extension of the context meta-model with privacy concepts and process mining concerns. Particularly, the **Behavioral Context** is extended and a **Privacy Context** is added. For our purpose, we adopt the XES event log meta-model [13] with the three main concepts *log*, *trace* and *event*. *Events* in an event log can be thought of as unique identifiers that carry a payload of *attributes*, similar to the rows of a table in which the attributes are columns. We assume that each event is assigned three mandatory attributes: `activity`, `time`, and `case`, which fulfills the three requirements for event data. Beyond that further information may be attached to the events of an event log, e.g., about the human (or non-human) resource that executed an activity. The Privacy Context includes *Privacy Policies* with several rules (access and collection rules), owned by *Data Providers* and *Data Consumers*. The *Data Controller* has to compare the policies of data consumers and providers to allow data transmission. In case of policy conflicts, the highest data protection restriction of one or more data providers wins (see Section 5 for an example) or legal regulations are superior and force implementation. To allow data providers to specify their privacy concerns, an easy understandable structure for privacy policies is needed. For this, we extend the five privacy elements described in [3](see Table 1): *What* specifies the set of information (attributes) which will be collected and it ensures to

track the connection between data providers and the activation of data source objects (e.g., wearables, devices) in the event log. *Collector* determines who is

Table 1. Ranges for Privacy Elements

Privacy Element	Data Provider	Data Consumer
Collector	a set of names or 'any'	single name
What	a list of data attributes	a list of data attributes
Aggregation	levels including time	levels including time
Retention Time	time frame and value	time frame and value
Purpose	'any' or certain purpose, level out of four ordered levels (no collection & no distribution, collection & (no dist. or limited dist. or dist.))	certain purpose, level
Recipient	empty	a set of names
Storage	a defined country, a certain continent, anywhere	country where the requested data will be stored
Legislation	a defined country, a certain continent, anywhere	country of legislation of the consumer

collecting the data. *Aggregation* is added for process mining purposes and defines the minimum levels of aggregation (e.g., on organizational units and time). The intention of introducing this element is to allow defining the starting point of data (re)use. If aggregation includes a level above 'no limit', anonymity must be ensured on data level. *Retention Time* defines how long the data will be stored within a certain time frame (days, weeks, months, unlimited). *Purpose* outlines a set of operational reasons for data access and storage. It consists of a set of <purpose, level> tuples allowing to specify prohibited purposes (black-list). Since several data providers should be allowed to specify their privacy preferences and to support the evaluation of privacy policies, we refine the notion of the *Purpose* element through purpose trees [6]. By the use of purpose trees we restrict the access to a certain purpose. In a purpose tree, each node represents a purpose (i.e., attributes defining reasons why such data should be accessed for) and edges represent a hierarchical relationships between them. In our use case, the company or the data controller has to define and maintain the purpose tree. The *Recipient* defines who gets data and is, thus, only relevant for the consumer. *Storage* specifies in which countries the data could be stored. In this way, the meta-model ensures data sovereignty. *Legislation* defines under which countries legislation data providers are willing to share their data. Both, *access rules* as well as *collection rules* include all of these privacy elements. To allow the *data provider* to see (1) which privacy design strategies are applied on their data and (2) which data was used by which other service including the privacy policy of the data consumer, the next section introduces a privacy preserving system architecture for process mining.

4.3 Architectural Model

The user-centered privacy-driven system relies on the eXtensible Access Control Markup Language (XACML)[5] which we adapted for our purpose. The language allows to evaluate access requests of data consumers according to the rules defined in policies (between e.g., the data provider and data controller) with the notions of:

- *Policy Enforcement Point (PEP):* It is the entry point for access requests. It inspects, requests, generates and sends an authorization request to the Policy Decision Point (PDP) and receives an authorization decision.
- *Policy Decision Point (PDP):* It matches the data provider and data consumer policies and returns an authorization decision.
- *Policy Information Point (PIP):* It acts as a source of data and can preprocess data before it is handed on to the PDP and PEP.
- *Policy Administration Point (PAP):* It allows the policy specification and management for different stakeholders.

Beside these notions the user-centered privacy-driven system consists of an *Information Portal*, *Data Collection Engine* and *Obligation Engine*, see Figure 4. The objective of an **Information Portal** is to provide a user friendly representation of stored data, data access attempts, the management of policies and foresee privacy preservation strategies for each stage (see Fig. 1). The objective of the **Data Collection Engine** is to collect data from heterogeneous data sources and to link them to attributes and persons. The **Obligation Engine** is responsible for keeping track of obligation triggers. This system architecture allows to (a) define and manage privacy policies, (b) determine more accurately who can do what with which data, (c) monitor compliance and (d) preview which privacy mechanisms are foreseen in which stages of process mining. Based on this architectural system we can evaluate the access requests as follows. In the set up process (stage 0, see Fig. 1) data controllers define purpose trees (e.g. together with the workers' council or union). Data controllers define privacy policies for data use purposes and data providers and consumers create their access and collection privacy policies in the information portal through the PAP. During stage 1 data is captured when tasks are committed. The *data collection engine* aligns the data to the potential collection policy and the *obligation engine* checks it for two issues: (1) whether data collection is allowed and can be directly used in stage 2 for the defined data use purpose, (2) whether this (event) data can be stored or not (conflict resolution), see stage 3. In case of storage approval, personal data is partitioned to reduce data correlations and contention. In stage 4 the data consumer requests a partial access to (event) data and logs through the PEP. The PDP compares each policy element of potential rules of the provider and consumer and decides whether access is granted through the PIP or not. These decisions are stored in a *request log*. According to the concept of user-centered system, which applies for our system design, relevant information (general data

[5] http://www.oasis-open.org/committees/xacml/

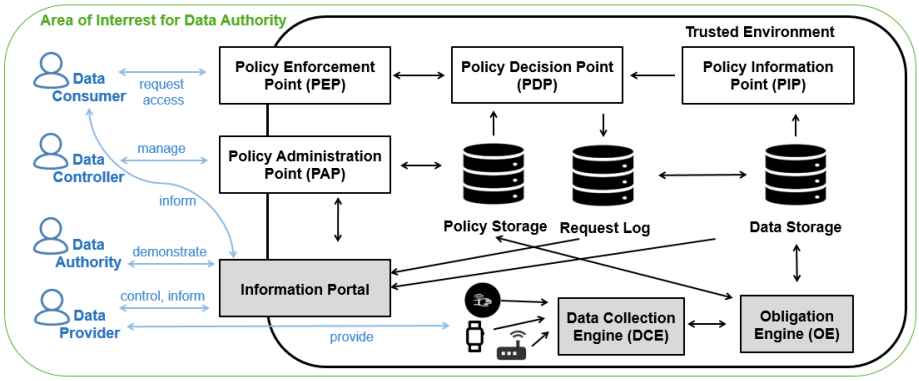

Fig. 4. User-Centered Privacy-Driven System relying on the eXtensible Access Control Markup Language. Information portal, request log, data collection engine and obligation engine were added in order to ensure privacy for process mining.

and event logs) about a data provider is accessible in the information portal in every stage (see Fig. 1). *Data providers* can read, update and delete privacy policies, track changes in the purpose trees and see which data consumers requested access to their data and to whom it was granted for both, the primary use and data (re)use. They can see in which aggregated representation their data was used. The *data authority* has access to the decisions and request logs as well. He can see all data and communication flows, the security mechanisms for the system and technical information such as encryption methods for data transmission and storage.

To sum up, the context meta-model defines information related to the privacy elements of the privacy preserving meta-model, especially the privacy elements 'What', 'Purpose' and 'Aggregate'. The meta-model is used as foundation to generate the information portal, the decision engine and the obligation engine[1]. The system design is capable to handle the IoT use case and process mining requirements. For instance, the collected data may lead to different fragments of logs having different policies, hence for a particular process mining associated with a given *purpose*, the system filters the collected data and build the log with only acceptable data accordingly.

5 Application of Strategies on the Meta-Model

In our example company ManuFuture Ltd, all production processes are monitored based on data collected from the manufacturing execution system (MES) but also from IoT-connected sensors and sensorised operators. Data providers (e.g., an operator) and data consumers (e.g., the quality assurance department) have defined their privacy policies related to a predefined purpose tree, e.g., as shown in Figure 5. Ann Jones, an operator of ManuFuture Ltd, has a rule for productivity and quality analysis using her data. Each privacy element of the rule

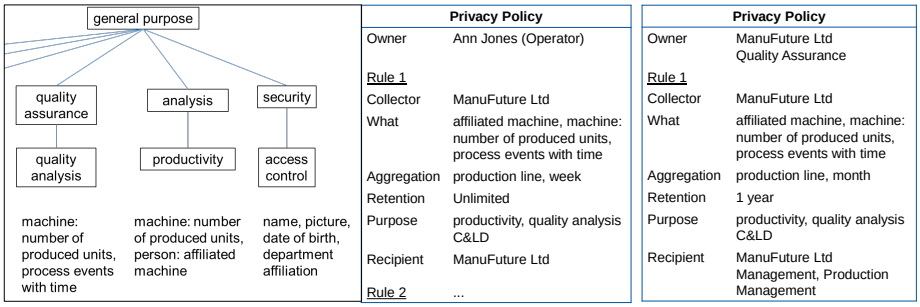

Fig. 5. Definition of a purpose tree and privacy policies for a company aiming to consider privacy.

is compared to each privacy element of the privacy policy of the data consumer quality assurance (QA) department of ManuFuture Ltd. The QA-department wants to hand over data to the management and production management regularly for the next year. Each privacy element is checked one by each other. Per month in 'Aggregation' is less restrictive that per week, in 'Retention' 1 year is included in unlimited, so the access would be granted to the data consumer. If for example aggregation of the data consumer would be e.g., on each machine or for each day, the access would not have been granted.

6 Conclusion and Future Work

Despite the advantage of IoT data for process mining, the increased amount of data brings also with it a high risk that what is disclosed may be private. Privacy cannot longer be neglected or considered as a marginal concern in the design of information systems. Privacy-by-design should be the standard. Relying on this, this paper considered an IoT manufacturing use case and aimed to design a system that preserve privacy for process mining. For this, we adopted an ABAC-based authorization model in order to support the eight privacy design strategies [12] for event logs. Beside the common components our system architecture consists of an information portal, data collection engine and an obligation engine. This allows to specify who does what, when, why, where and how with your own personal data in the IoT context and during process mining.

References

1. Adam, K., Netz, L., Varga, S., Michael, J., Rumpe, B., Heuser, P., Letmathe, P.: Model-Based Generation of Enterprise Information Systems. In: EMISA. CEUR Workshop Proc., vol. 2097, pp. 75–79 (2018)
2. Agrawal, D., Aggarwal, C.C.: On the design and quantification of privacy preserving data mining algorithms. In: PODS 2001. ACM Press (2001)

3. Allison, D.S., El Yamany, H.F., Capretz, M.: Metamodel for privacy policies within soa. In: ICSE WS on SE for Secure Systems (2009). pp. 40–46. IEEE (2009)
4. Basso, T., Montecchi, L., Moraes, R., Jino, M., Bondavalli, A.: Towards a uml profile for privacy-aware applications. In: IEEE Int. Conf. on Computer and Information Technology. pp. 371–378 (2015)
5. Bergeron, E.: The difference between security and privacy (2000), https://www.w3.org/P3P/mobile-privacy-ws/papers/zks.html
6. Byun, J.W., Bertino, E., Li, N.: Purpose based access control of complex data for privacy protection. In: 10th ACM Symposium on Access Control Models and Technologies. pp. 102–110. SACMAT '05, ACM (2005)
7. Colesky, M., Caiza, J.C., Alamo, J.M.D., Hoepman, J.H., Martín, Y.S.: A system of privacy patterns for user control. In: SAC 2018. ACM Press (2018)
8. van Eck, M.L., Lu, X., Leemans, S.J.J., van der Aalst, W.M.P.: PM^2 : A process mining project methodology. In: Advanced Information Systems Engineering, pp. 297–313. Springer International Publishing (2015)
9. European Union: Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (GDPR). Official Journal of the European Union **L119**, 1–88 (2016)
10. Feltus, C., Grandry, E., Kupper, T., Colin, J.N.: Model-driven approach for privacy management in business ecosystem. In: 5th Int. Conf. on Model-Driven Engineering and Software Development. pp. 392–400. INSTICC, SciTePress (2017)
11. Grace, P., Surridge, M.: Towards a model of user-centered privacy preservation. In: Int. Conf. on Availability, Reliability and Security (ARES). p. 91 pp. ACM (2017)
12. Hoepman, J.H.: Privacy design strategies. In: Cuppens-Boulahia, N., Cuppens, F., Jajodia, S., Abou El Kalam, A., Sans, T. (eds.) ICT Systems Security and Privacy Protection. pp. 446–459. Springer Berlin Heidelberg (2014)
13. IEEE: Standard for extensible event stream (XES) for achieving interoperability in event logs and event streams. Standard, IEEE (2016)
14. Liu, C., Duan, H., ZENG, Q., Zhou, M., Lu, F., Cheng, J.: Towards comprehensive support for privacy preservation cross-organization business process mining. IEEE Transactions on Services Computing (2016)
15. Mannhardt, F., Bovo, R., Oliveira, M.F., Julier, S.: A taxonomy for combining activity recognition and process discovery in industrial environments. In: Intelligent Data Engineering and Automated Learning. pp. 84–93. LNCS, Springer (2018)
16. Mannhardt, F., Petersen, S., Fradinho Duarte de Oliveira, M.: Privacy challenges for process mining in human-centered industrial environments. In: Intelligent Environments 2018. IEEE Xplore (2018)
17. Michael, J., Steinberger, C.: Context modeling for active assistance. In: ER Forum and the ER Demo Track. pp. 221–234 (2017)
18. Rozinat, A.: Process Mining: Conformance and Extension. Ph.D. thesis, Eindhoven University of Technology, Eindhoven (2010)
19. Rozinat, A., Günther, C.W.: Privacy, Security and Ethics in Process Mining. Tech. rep., Fluxicon (2016), https://bit.ly/2QZ9Pxk
20. Stocker, T., Accorsi, R.: Secsy: A security-oriented tool for synthesizing process event logs. In: Proceedings of the BPM Demo Sessions 2014. p. 71 (2014)
21. Wang, L., Wijesekera, D., Jajodia, S.: A logic-based framework for attribute based access control. pp. 45–55. FMSE '04, ACM (2004)
22. Xu, L., Jiang, C., Qian, Y., Ren, Y.: The Conflict Between Big Data and Individual Privacy. Springer (2018)