Facilitating GDPR compliance

Facilitating GDPR compliance: the H2020 BPR4GDPR approach

Georgios V. Lioudakis[1], Maria N. Koukovini[1], Eugenia I. Papagiannakopoulou[1], Nikolaos Dellas[2], Kostas Kalaboukas[2], Renata Medeiros de Carvalho[3], Marwan Hassani[3], Lorenzo Bracciale[4], Giuseppe Bianchi[4], Adrian Juan-Verdejo[5], Spiros Alexakis[5], Francesca Gaudino[6], Davide Cascone[6], and Paolo Barracano[7]

[1] ICT abovo P.C., Iridanou 20, 11528, Athens, Greece
[2] SingularLogic S.A., Achaias 3 & Trizinias, 14564, N. Kifisia, Greece
[3] Eindhoven University of Technology, De Groene Loper 5, Eindhoven, Netherlands
[4] University of Rome "Tor Vergata", Via del Politecnico 1, 00133 Rome, Italy
[5] CAS Software AG, CAS Weg 1-5, 76131, Karlsruhe, Germany
[6] Baker McKenzie, Piazza Filippo Meda 3, 20121, Milano, Italy
[7] Innovazioni Tecnologiche SRL, Via Arcidiacono Giovanni 43, 70124 Bari, Italy

Abstract. This paper outlines the approach followed by the H2020 BPR4GDPR project to facilitate GDPR compliance. Its goal is to provide a holistic framework able to support end-to-end GDPR-compliant intra- and inter-organisational ICT-enabled processes at various scales, while also being generic enough, fulfilling operational requirements covering diverse application domains. To this end, solutions proposed by BPR4GDPR cover the full process lifecycle addressing major challenges and priorities posed by the Regulation.

Keywords: GDPR compliance, data protection, process management, privacy-aware access and usage control, process mining

1 Introduction

The digital revolution has resulted in a lag between regulations and the current reality of the social media, Cloud Computing, Internet of Things, Big Data, to mention a few trends that didn't exist merely two decades ago and have resulted in increasingly interconnected systems, amazing processing power (and results thereof), and data proliferation. As dependency to technology increases, so do the information trails left behind following daily activities of people. To this end, the General Data Protection Regulation (GDPR) [1] comprises a milestone step towards filling the "regulatory gap", creating an environment able to cope with the technological and business reality, and provide for the protection of privacy.

Apart from the mandate for GDPR compliance—and the non-neglectable financial penalties, compliance is motivated also by the market needs, particularly the growing people awareness and their increasing demand that companies protect their information [7]. For example, the 2015 TalkTalk privacy breach resulted in over 100.000 customers' loss and costs of £60m [9].

However, organisations declare difficulties in GDPR provisions' implementation, despite the resources and money spent, whereas particular problems are faced as regards the new requirements GDPR introduces. The challenges, either technical or organisational, include, among others: interpretation of GDPR requirements; operational adaptation towards privacy-aware and compliant business practices; holistic data views and processing actions inventory; enforcement of security means; management of the relations with third parties and the data subjects, and enforcement of rights thereof; last but not least, significant resources are required and, whereas big companies may have money and resources to invest, both human and monetary, this does not necessarily apply for SMEs.

The H2020 BPR4GDPR project[1] aims at bringing about a new GDPR compliance paradigm, by providing the tools and methodologies that will significantly facilitate the implementation of the appropriate technical and organisational measures, particularly by SMEs, to ensure that data collection and processing is performed in accordance with the GDPR. The BPR4GDPR compliance approach consists in automatically re-engineering workflows, being business processes or low-level service compositions, so that they become compliant *by design*, whereas enforcement will be supported by an easy to deploy "compliance toolkit", providing the fundamental common functions for cryptography, access management, and enforcement of data subjects' rights. Further, the overall organisational compliance and underlying systems' behaviour will be governed by a comprehensive policy-based access and usage control framework, conceived on the basis of the GDPR and managing all requirements thereof. Finally, BPR4GDPR will opt for enabling BPR4GDPR solutions deployment on the Cloud, therefore providing for Compliance-as-a-Service (CaaS).

This paper describes the BPR4GDPR approach towards facilitating GDPR compliance. It is organised as follows: Section 2 outlines the operational phases towards an holistic approach to GDPR compliance, whereas Section 3 provides an overview of the technical architecture of the project. The paper concludes with an outlook on the BPR4GDPR innovation potential.

2 BPR4GDPR operational phases

As illustrated in Fig. 1, there are six main stages comprising the BPR4GDPR process lifecycle, numbered 1–6; they respectively deal with its specification by an administrative user or its discovery based on event logs, its analysis and redesign, implementation, execution and monitoring, resulting eventually in possibly updated process models, adapted to real-time circumstances and other evolutionary factors. Furthermore, BPR4GDPR considers two additional phases, vertical to the process lifecycle and devised, respectively, for the initial actions that should take place in order for an organisation to become BPR4GDPR-ready (phase 0), and for the operations that are either horizontal, or process-independent (phase 7). The eight phases are summarised in the following.

[1] H2020 BPR4GDPR: Business Process Re-engineering and functional toolkit for GDPR compliance, contract number 787149, http://www.bpr4gdpr.eu/

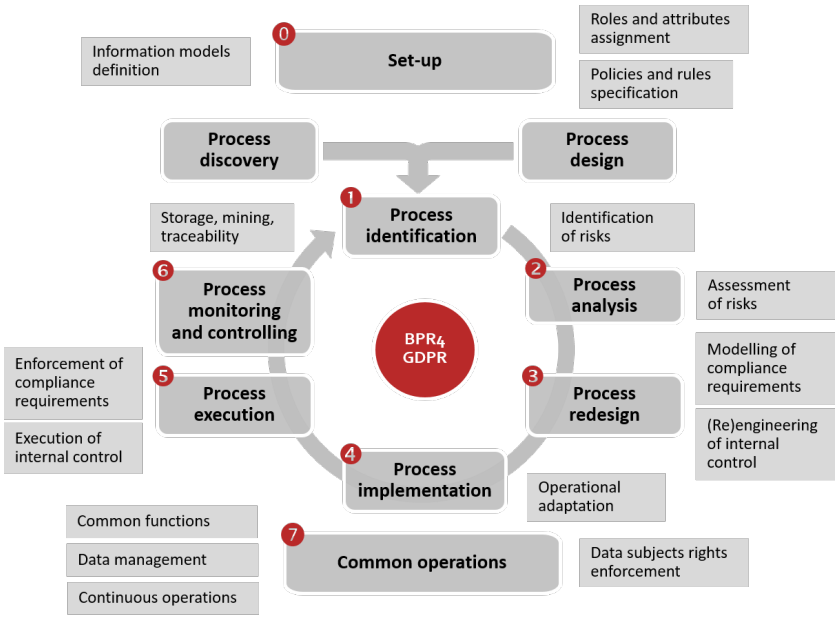

Fig. 1: BPR4GDPR operational phases.

Phase 0: Set-up This phase consists in all tasks that concern setting up the base elements of the BPR4GDPR operation and performance of all preparatory activities that are fundamental for the whole system to work. These include, for instance, the specification of the information models, the classification of data and other resources, the assignment of roles and attributes to the different entities —human and others— participating in the system, the definition of purposes behind data collection and processing, and the specification of policies and underlying rules that should govern the operation of the system components.

Phase 1: Process identification This phase concerns the definition of process models, leveraging two possible ways: i) process discovery mechanisms, in order to depict the procedures and associated information flows taking place within an organisation, through the resulting process models; ii) definition of procedures by administrative users, using the appropriate graphical tool. Either way, the outcome will be process model specifications providing for the incorporation, by later phases, of sophisticated constraints enforceable at run-time.

Phase 2: Process analysis This concerns the analysis of a process model in order to identify the risks, flaws and points of non-compliance, on the basis of well-defined policies. This way, process models shall be evaluated and verified as regards their compliance with the GDPR and provisions thereof. This phase entails a highly expressive policy framework, considering a variety of aspects and parameters, such as attributes, context, dependencies between actions and participating entities therein, as well as separation and binding of duty constraints.

Phase 3: Process redesign This phase complements process analysis, by providing for the automatic transformation of non-compliant process models,

so that they are rendered inherently privacy-aware before being deployed for execution. It is supported by a Compliance Metamodel, a comprehensive process modelling technology able to capture advanced privacy provisions, and a fundamental goal of the project.

Phase 4: Process implementation This concerns the effective enactment of GDPR-compliant processes, mainly as regards two aspects. The first reflects the requirement for availability of necessary mechanisms for the enforcement of privacy provisions. To this end, a comprehensive set of tools is needed, able to support the diverging requirements that may arise from GDPR (data handling, data subjects' involvement, various PETs, etc.). The second aspect is related to the structural and semantic alignment of the modelled processes with the actual infrastructure of the organisation; this shall be grounded primarily on the semantic foundations of the project, which will enable the refinement and adaptation of the BPR4GDPR models to each organisation's reality.

Phase 5: Process execution This extends process implementation by ensuring the execution of processes in accordance to compliant process and following the appropriate configuration set forth during the process implementation phase. In other words, it is mainly during this phase when the mechanisms towards real-time privacy protection are applied and respective provisions are enforced.

Phase 6: Process monitoring and controlling This phase concerns the use of process mining for the ex post analysis of processes, in order to ensure that specified policies are indeed enforced, fostering accountability. Furthermore, and apart from verifying compliance, such techniques will offer the added value of automatically improving process models over time towards optimised fulfilment of both legal and business goals and requirements.

Phase 7: Common operations This refers to operations that are not (necessarily) part of a process lifecycle, but are rather executed asynchronously to processes or are independent thereof. They fall in different categories, including: i) Functions that are supportive to all phases and other organisational activities (e.g., authorisation mechanisms); ii) enforcement of certain data subject rights, such as synchronous and asynchronous consent and management of privacy preferences, access to data, erasure, portability, etc.; iii) general data management functions, such as secure data storage and enforcement of retention provisions; iv) continuous operations, such as risk estimation, operations logging, etc.

3 Architecture

In order to cover its functional needs towards GDPR compliance and cope with the operational phases described in Section 2, BPR4GDPR has specified the system architecture highlighted in Fig. 2. As illustrated, the BPR4GDPR architecture is divided in four "quadrants", reflecting different groups of functionalities.

Governance provides all functions related to the specification of policies and reasoning thereof, thus representing the Policy Decision Point (PDP) of the system. **Planning** concerns the specification of workflow models and their

verification as regards compliance with the GDPR and their subsequent transformation, if needed, so that they become compliant *by design*. **Monitoring** deals with process mining and monitoring with the aim to identify discrepancies between compliant and actual behaviour. Finally, **Run-time** provides the means for the run-time system operation, particularly in terms of policy enforcement, data management, privacy-enhancing tools, and interaction with data subjects. The following sections summarise the main principles and technical ideas.

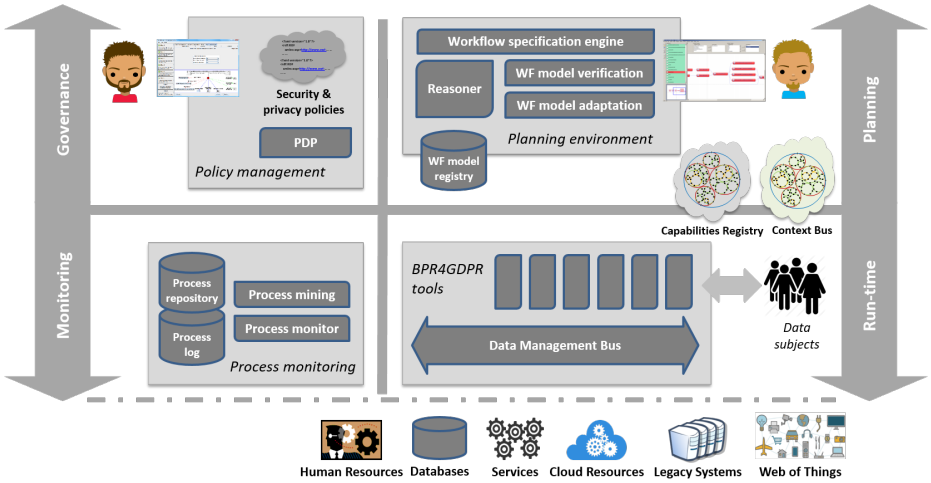

Fig. 2: BPR4GDPR architecture.

3.1 Governance

Policies are spotlighted at the core of the BPR4GDPR framework, as they comprise the drivers for the compliance-aware process verification and re-engineering, as well as for the run-time operation, providing the behavioural norms of underlying entities. Privacy and security policies are incorporated in the processes already during their specification through the Compliance Metamodel (cf. Section 3.2) or during the verification and transformation phase as a result of the compliance checks. Run-time enforcement is achieved through the Compliance Toolkit (Section 3.4), with policies regulating access to and usage of the underlying resources and prescribing the employment of privacy-enhancing mechanisms.

In that respect, BPR4GDPR focuses on providing a comprehensive framework for the specification of sophisticated security and privacy policies, able to capture all complex concepts stemming from the GDPR and other related legislation, and the needs and requirements of all associated stakeholders. Eventually, and fostering legislation-awareness, BPR4GDPR is specifying a Compliance Ontology providing a high-level codification of GDPR into concepts that need to be taken into consideration by the policy framework, as well as in the context of privacy-aware process re-engineering. The Compliance Ontology includes, for

instance, the types under which personal data fall, roles of the entities requesting and processing personal data, operations and services performed over personal data, attributes of all entities, purposes of requesting/processing data, among others. It also considers the interrelations among identified concepts and provides for their thorough semantic structuring, by specifying hierarchies reflecting generalisation/particularisation and the inclusion of some types to another.

The Compliance Ontology is extended with policies, formalised as sophisticated and fine-grained access and usage control rules. For the specification of the latter, BPR4GDPR will deliver a comprehensive Policy-based Access and Usage Control framework, tailored for the needs of highly distributed environments, involving multiple stakeholders, even in cross-border scenarios. The ground technology is the academic work described in [19], along with the respective software prototype. The Policy Model Ontology (PMO) introduced in [19] consists of two parts: the Information Model, semantically representing the domain entities, and a highly expressive rule-based policy framework. Its expressiveness allows the specification complex interrelations and dependencies between loosely-related actions and the enforcement of Separation and Binding of Duty (SoD/BoD) constraints [4], while hierarchies provide for comprehensive and simpler specification and formalisation of fine-grained security and data protection requirements, at any level of abstraction. The resulting policies will allow for attribute-based data collection and overall handling, and managing all associated constraints, including retention periods and the application of protection measures.

3.2 Planning

A vital step towards any organisation's regulatory compliance is the accurate modelling of privacy-aware processes, offering precise insight into what is being or must be executed as part of the corresponding operational procedures. For this purpose, the appropriate tools are needed, on the one hand, allowing their description in a way that effectively guides their execution and integration into the organisational environment, and, on the other, being expressive enough, in order to be able to capture the associated provisions and incorporate comprehensive security and privacy policies in their design.

Given that a process can be roughly seen as coordination of tasks, i.e., operational steps, towards the fulfilment of a more complex business objective, said policies must consist in accurately specifying who performs which operation on which resource during each such step, but also on the information exchanged towards their coordination. Going a step further, in order to achieve adequate expressiveness, additional concepts need to be reflected in the resulting process models, complementing the basic features of tasks and information flow; these include, the use of attributes in the description of all participating entities, as well as context- and situation-awareness, that have been recognised as key enablers in the enforcement of security policies in general [6], providing for the required flexibility and adaptability levels in view of emerging threats. Finally, specific security aspects often pertaining to process execution, like SoD/BoD [4],

the data state at each process step (e.g., encrypted vs. unencrypted) and various other kinds of interrelations among process elements need to also be considered.

In order to achieve the above, BPR4GDPR is grounded upon a **Compliance Metamodel**, with a view to formally incorporating sophisticated GDPR-oriented provisions. This is based on prior academic work of BPR4GDPR researchers [15], and presents a number of innovative features, including: i) it enables the comprehensive specification of workflow elements, providing extensive coverage of core workflow perspectives [12]; ii) it introduces the novel concept of *assets*, as a means for representing the entities being subject to the execution of workflow tasks; iii) it allows the explicit modelling of both control and data flows, thus being suitable for applications based on either of them or both of them combined; iv) its expressiveness supports the expression of complex and varying security and privacy constraints.

Every process model must be rendered GDPR-compliant before being enacted within the organisation, and this must take place transparently to the user, i.e., the policies being part of its specification, as described above, must be automatically incorporated as part of its design. Therefore, apart from the comprehensive definition of process models, the BPR4GDPR approach involves sophisticated means for the evaluation of a process specification against a number of compliance aspects. Their main aim is, on the one hand, to control access to, usage of, and flow of information and prevent illegitimate activity, e.g., disclosure of data to unauthorised entities, and, on the other, to determine whether critical tasks are properly included and, if not, impose their execution, referring, for example, to cryptographic operations that must be performed on data before their transfer or storage, approval that must be granted before privacy-sensitive operations, etc. Only after a process has been successfully evaluated against said compliance aspects, may be available for future deployment and execution.

3.3 Monitoring

In the last two decades the focus on process-orientation (e.g., process-aware information systems or BPM systems) has increased, while, with the incredible growth of event data (cf. "Big Data"), it has become possible to use process mining, i.e., a posteriori analysis techniques exploiting the information recorded in the event logs, to discover models and check the conformance of existing ones. Indeed, most organisations have very limited knowledge about the reality happening throughout their day-to-day operation; process mining focuses on this kind of problem, with a view to assessing the organisational reality and reduce the gap between what is supposed to happen and what actually happens. The key facets of process mining are discovery, monitoring and improvement of real processes by extracting knowledge from the organisation's available data. Previous research has pointed large discrepancies between the idealized model and the process in reality. Moreover, process mining has shown that different models are possible for different and particular views on the process at hand.

In light of the above, BPR4GDPR implements a Privacy-Aware Process Mining Framework, based on mature technology brought by the Analytics for In-

formation System Group at Eindhoven University of Technology, particularly ProM[2] [2][13][16]. By using ProM, BPR4GDPR seeks to meet requirements related to: *(i)transparency*– being able to discover and integrate interpretable business procedures into a process model, i.e., to generate process models reflecting, as precisely as possible, an organisation's current modus operandi; *(ii) compliance*– automatically identifying "business rules" for different perspectives; and *(iii) accountability*– spotting non-conformant executions. While checking the conformance between a process model and events in reality, two main concepts should be considered: *real-time data* and *concept drift*.

Streaming process mining techniques [10] can process real-time data in reasonable time. As a result, the modelled process can be used to find the differences between designed and actual models, detecting problems, anomalies and potential frauds. The end result of this effort will be a real-time process mining technique [11][22] to enable, for example, early warning in automated processes or finding errors or misuse regarding the defined policies.

For non-stationary domains, business rules may become less accurate over time (a concept drift problem) or new factors/requirements may arise, so that the process model will be out-of-date and in need to be adapted/improved. To this end, both active and passive solutions will be provided. The former type will define a *change-detection system* that will update the statistics about the data-related behaviours and will establish rules to integrate recent information to improve the model. The latter will offer *continuous update*, frequently retraining the model based on the most recent observations. Approaches from *static* conformance checking [5] have been tested for compliance requirements checking [21], however, these attempts did not target process model repair [8] in the real time. BPR4GDPR will advance the state-of-the-art compliance checking approaches in this direction.

Checking *a posteriori* the compliance of running processes will help to identify discrepancies between modelled and observed behaviour, but also follow and guide process evolution over time, for the benefit not only of legality but also of the affected businesses per se. This becomes even more important considering that such findings may be correlated with other data sources, various context and KPIs, in order to expose vulnerabilities not foreseen at the model level, but also extract information that can only occur through day-to-day practice.

3.4 Run-time

In order to facilitate the deployment of appropriate technical measures, as required by the Regulation, BPR4GDPR is developing a set of functional components addressing common needs of stakeholders. This so-called **Compliance Toolkit** consists of modular functions that, fostering "plug and play" to the extent possible, will be easy to deploy, easy to configure and easy to integrate within an organisation's ICT environment, while they will be automatically incorporated to process chains, as a result of re-engineering. The toolkit is complemented by a Capabilities Registry, providing information regarding availability

[2] http://www.promtools.org/

of the capabilities of the underlying tools, and a Context Bus, that keeps track of the real-time contextual parameters and events. The modules of the Compliance Toolkit fall into three broad families, described in the following.

Privacy-enhancing technologies (PETs) These refer particularly to cryptographic tools, devised for anonymisation and pseudonymisation, data and communications confidentiality, message and information integrity, non-repudiation, as well as enforcement of access rights by cryptographic means. BPR4GDPR leverages open state-of-the-art tools, as well as prior research results of its partners, such as the advanced cryptographic functions developed in the context of the ReCRED project[3]. To this end, BPR4GDPR employs plethora of cryptographic primitives, both symmetric and asymmetric, together with data-centric techniques, particularly Attribute-Based Encryption (ABE) [3], that allows ciphering data with one or more *attributes* that the recipient has to possess.

As regards anonymisation and pseudonymisation, special attention is needed in order to deal with modern de-anonymisation attacks [18]. With the goal to find a trade-off between data usability and the potential privacy risks, BPR4GDPR leverages a rich set of respective techniques, ranging from legacy, e.g., hashing, to state-of-the-art open mechanisms, such as l-diversity, t-closeness and k-anonymity, and "secure queries" [17]. The more suitable mechanism, or combination thereof, is selected at run-time in an ad hoc manner.

Data management tools These are devised for controlling data handling, by means of data access and usage management, including management of retention and storage, pre- and post-processing, etc. A core position is held here by the Data Management Bus (DMB) (Fig. 2), comprising the main Policy Enforcement Point (PEP) of the run-time environment. It is a policy-driven data management and messaging middleware, able to control data collection, processing, storage and dissemination in a fine-grained way, and to handle data flows in a compliant manner. The DMB constitutes the interoperation Bus among all other tools of the Toolkit, also orchestrating their inter-working towards the application of data protection means. It provides a unified solution for accessing information stored in heterogeneous systems, under a common interface, while providing common, semantic abstractions of underlying components' operational aspects.

User-centered tools The GDPR includes a wide range of existing and new rights for the data subjects, while requiring controllers to provide significantly more information to data subjects about their processing activities and to take into consideration of data subjects' preferences as regards data handling. To this end, this type of tools provides for the enforcement of data subjects' rights, including: information and notification; consent management and consideration of own data handling preferences; rights of access, erasure ("right to be forgotten") and rectification; right to data portability.

[3] H2020 ReCRED, From Real-world Identities to Privacy-preserving and Attribute-based CREDentials for Device-centric Access Control, https://www.recred.eu/

4 Outlook: the BPR4GDPR innovation potential

The privacy technology market is rapidly maturing to meet the needs of organisations around the world. The features that most noteworthy products offer can be roughly categorised in the following: a) compliance assessment and high-level incident response, mainly through diagnostic, after-the-fact observation, sometimes enhanced with appropriate data management capabilities, b) consent management, c) other enforcement tools, related to, e.g., de-identification/pseudonymity. Interestingly, very few seem to adequately cover all three categories; further, they are either domain-specific or rather generic, in the latter case raising questions about their thoroughness and effective deployment in any organisational setting. Finally, process orientation has not been extensively incorporated in current offerings. Besides, as observed in [14], even BPM software encompassing so-called governance, risk and compliance (GRC) functionality is mostly limited to the definition of compliance requirements and to explicitly imposing protection mechanisms during execution, while automated compliance checking, let alone enforcement, does not seem to be state-of-the-art.

BPR4GDPR addresses the above shortcomings by providing a holistic, yet modular, solution supporting privacy-by-design throughout the entire lifecycle of an organisational process, based collectively on innovative approaches on all the above-identified points. Specifically, BPR4GDPR focuses on business processes and is grounded on the core GDPR provisions, with a view to addressing essentially, in broader legal terms, the four major aspects of privacy according to Solove's reference taxonomy [20], namely information *collection*, *processing*, *dissemination* and *invasion*, tightly intertwined with the roles of data subjects and data holders. To this end, project innovation is distributed through process lifecycle as follows:

Process discovery BPR4GDPR is using process mining targeted specifically at making privacy–aware workflows. The goal of process mining is to extract information from event logs, i.e., process mining describes a family of *a posteriori* analysis techniques exploiting the information recorded in the event logs. Typically, these approaches assume that it is possible to sequentially record events such that each event refers to an activity and is related to a particular case (i.e., a process instance). Furthermore, some mining techniques use additional information such as the performer or originator of an event, its timestamp, or data elements recorded with the event. As a first step towards helping organisations to be compliant, BPR4GDPR employs process mining in order to generate process models reflecting, as precisely as possible, their current modus operandi. Process discovery constitutes the evolution, at large scale, of data discovery, that is already being provided by various offerings, into the automatic identification of privacy-sensitive processes, as a response to the increasingly complex and distributed information flows.

Process analysis and redesign Automatic process verification with respect to GDPR provisions is essential, taking into consideration issues of expertise but also administrative costs involved. BPR4GDPR expects to outweigh existing ap-

proaches in that it incorporates additional aspects to verify, but also transform workflow designs every time this is necessary to ensure secure enactment. This is founded on: a) novel means for the incorporation into a workflow specification of all kinds of provisions that may be dictated by the GDPR; although approaches on the annotation of business processes with policies already exist, the innovation of BPR4GDPR consists in the detail level and variety of requirements it is be able to express, as well as in the balanced handling of all three core workflow perspectives, namely control, data and resource, that are of equal importance to privacy; b) a highly expressive access and usage control model, that, being defined primarily following the GDPR, is also tailored to process management needs, incorporating associated requirements at an extraordinary level of detail; a key contribution is the ability to enforce access and usage control taking into consideration large-scale associations of operations, rather than being limited to the execution of individual tasks. Further, the implications arising in collaborative scenarios in view of inter-domain business processes are also addressed.

Process implementation and execution During process run time, the Compliance Toolkit provides novel tools covering the entire spectrum of enabling technology required for the enforcement of core GDPR provisions, including cryptography, data handling and notification mechanisms, and user-centered tools ensuring consent, as well as the exercise of other data subjects' rights. It must be noted that BPR4GDPR will be extensible and thus enforceable to its full potential to any domain and organisation type thanks to its semantic foundations and the guidelines it will provide towards successfully deploying, on the one hand, the re-engineered, GDPR-enhanced processes and, on the other, the BPR4GDPR tools within each already existing operational environment.

Process monitoring and controlling BPR4GDPR is also the first to exploit process mining techniques for *a posteriori* compliance check of running GDPR-compliant processes, in order to identify discrepancies between modelled and observed behaviour, and both follow and guide process evolution over time. These findings may also be correlated with other data sources, various context and KPIs (customer satisfaction, cost, etc.) in order to expose vulnerabilities not foreseen at the model level, but also extract information that can only occur through day-to-day practice.

Acknowledgment

This research is being supported by the European Commission, in the frame of the H2020 BPR4GDPR project (Grant No. 787149). The authors would like to express their gratitude to the Consortium for the fruitful discussions.

References

1. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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 (General Data Protection Regulation) (May 2016)
2. van der Aalst, W.M.P., et al.: Prom: The process mining toolkit. In: Proceedings of the Business Process Management Demonstration Track (BPMDemos 2009), Ulm, Germany, September 8, 2009 (2009)
3. Bethencourt, J., Sahai, A., Waters, B.: Ciphertext-policy attribute-based encryption. In: 2007 IEEE Symposium on Security and Privacy (SP '07) (May 2007)
4. Botha, R.A., Eloff, J.H.P.: Separation of duties for access control enforcement in workflow environments. IBM Systems Journal 40(3), 666–682 (March 2001)
5. Carmona, J., et al.: Conformance Checking - Relating Processes and Models. Springer (2018)
6. Cuppens, F., Cuppens-Boulahia, N.: Modeling Contextual Security Policies. International Journal of Information Security 7(4), 285–305 (2008)
7. European Commission, Directorate-General for Communication: e-privacy, Flash Eurobarometer 443 (December 2016)
8. Fahland, D., van der Aalst, W.M.P.: Model repair - aligning process models to reality. Inf. Syst. 47, 220–243 (2015)
9. Farrell, S.: Talktalk counts costs of cyber-attack, The Guardian. https://bit.ly/2hjiKYE (February 2016)
10. Hassani, M.: Efficient clustering of big data streams. Ph.D. thesis, RWTH Aachen University, Germany (2015)
11. Hassani, M., et al.: Efficient process discovery from event streams using sequential pattern mining. In: IEEE Symposium Series on Computational Intelligence, SSCI 2015, Cape Town, South Africa, December 7-10, 2015. pp. 1366–1373 (2015)
12. Jablonski, S., Bussler, C.: Workflow management: modeling, concepts, architecture and implementation. International Thomson Computer Press (1996)
13. Kalenkova, A.A., de Leoni, M., van der Aalst, W.M.P.: Discovering, analyzing and enhancing BPMN models using ProM. In: Proceedings of the BPM Demo Sessions 2014 (2014)
14. Koetter, F., Kochanowski, M., Drawehn, J.: Governance, risk and compliance in BPM - a survey of software tools. In: The 5th International Conference on Business Intelligence and Technology (BUSTECH 2015) (March 2015)
15. Koukovini, M.N.: Inherent privacy awareness in service-oriented architectures. Ph.D. thesis, National Technical University of Athens (2014)
16. Mans, R., van der Aalst, W.M.P., Verbeek, H.M.W.E.: Supporting process mining workflows with rapidprom. In: Proceedings of the BPM Demo Sessions 2014 (2014)
17. Mirkovic, J.: Privacy-safe network trace sharing via secure queries. In: Proceedings of the 1st ACM Workshop on Network Data Anonymization (NDA '08) (2008)
18. Narayanan, A., Shmatikov, V.: Robust de-anonymization of large sparse datasets. In: 2008 IEEE Symposium on Security and Privacy (SP 2008) (May 2008)
19. Papagiannakopoulou, E.I.: Semantic Access Control Model for Distributed Environments. Ph.D. thesis, National Technical University of Athens (2014)
20. Solove, D.J.: A taxonomy of privacy. University of Pennsylvania Law Review 154(3), 477–560 (January 2006)
21. Taghiabadi, E.R., et al.: Compliance checking of data-aware and resource-aware compliance requirements. In: On the Move to Meaningful Internet Systems: OTM 2014 Conferences - Confederated International Conferences: CoopIS, and ODBASE 2014, Amantea, Italy, October 27-31, 2014, Proceedings. pp. 237–257 (2014)
22. van Zelst, S.J., et al.: Online conformance checking: relating event streams to process models using prefix-alignments. International Journal of Data Science and Analytics (Oct 2017)