# Facilitating GDPR Compliance: The H2020 BPR4GDPR Approach

Georgios V. Lioudakis, Maria N. Koukovini, Eugenia I. Papagiannakopoulou, Nikolaos Dellas, Kostas Kalaboukas, Renata Carvalho, Marwan Hassani, Lorenzo Bracciale, Giuseppe Bianchi, Adrian Juan-Verdejo, et al.

# 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
georgios.lioudakis@ict-abovo.gr, mariza.koukovini@ict-abovo.gr, eugenia.papagiannakopoulou@ict-abovo.gr
[2] SingularLogic S.A., Achaias 3 & Trizinias, 14564, N. Kifisia, Greece
kkalaboukas@singularlogic.eu, nikolaos.dellas@gmail.com
[3] Eindhoven University of Technology, De Groene Loper 5, Eindhoven, Netherlands
R.Medeiros.de.Carvalho@tue.nl, M.Hassani@tue.nl
[4] University of Rome "Tor Vergata", Via del Politecnico 1, 00133 Rome, Italy
lorenzo.bracciale@uniroma2.it, giuseppe.bianchi@uniroma2.it
[5] CAS Software AG, CAS Weg 1-5, 76131, Karlsruhe, Germany
adrian.juan@cas.de, Spiros.Alexakis@cas.de
[6] Baker McKenzie, Piazza Filippo Meda 3, 20121, Milano, Italy
Francesca.Gaudino@bakermckenzie.com, Davide.Cascone@bakermckenzie.com
[7] Innovazioni Tecnologiche SRL, Via Arcidiacono Giovanni 43, 70124 Bari, Italy
P.Barracano@intempra.com

**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 General Data Protection Regulation (GDPR) [1] comprises a milestone in data protection, creating an environment able to cope with the technological and business reality, and provide for the protection of privacy. However, organisations declare difficulties in GDPR implementation, despite the resources and money spent, The challenges, either technical or organisational, include, among others: interpretation of GDPR requirements; operational adaptation towards

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 resources to invest, this does not necessarily apply for SMEs.

This paper presents the approach followed by the H2020 BPR4GDPR project[1], towards a new GDPR compliance paradigm. BPR4GDPR is building tools for facilitating the implementation of the appropriate 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 is supported by an easy to deploy "compliance toolkit", providing the fundamental common functions for cryptography, access management, and enforcement of data subjects' rights. In the following, 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.

## 2 BPR4GDPR operational phases

The BPR4GDPR process lifecycle (Fig. 1) consists of six main stages, numbered 1–6, dealing with process design or discovery, its analysis and re-design, implementation, execution and monitoring. Two additional phases, vertical to the process lifecycle, are devised for the initial "set-up" actions (Phase 0) and for the operations that are either horizontal, or process-independent (Phase 7). The eight phases are summarised in the following.

**Phase 0: Set-up** This consists in setting up the base elements for system operation. These include the specification of the information models, the classification of data and other resources, the assignment of roles and attributes, the definition of purposes behind data collection and processing, and the specification of policies and rules that should govern the system operation.

**Phase 1: Process identification** This concerns the definition of process models, by: i) process discovery mechanisms, based on process logs; ii) definition of procedures 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 policy-based analysis of a process model in order to identify the risks, flaws and points of non-compliance. This way, process models shall be evaluated and verified as regards their compliance

[1] H2020 BPR4GDPR: Business Process Re-engineering and functional toolkit for GDPR compliance, contract number 787149 (01/05/2018 – 30/04/2021) http://www.bpr4gdpr.eu/

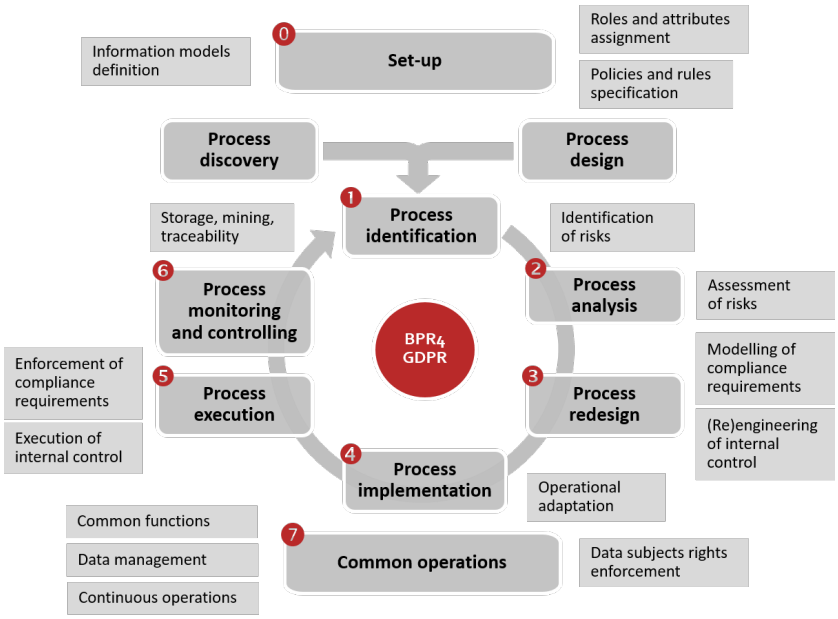


Fig. 1: BPR4GDPR operational phases.

with the GDPR . This phase entails a highly expressive policy framework, considering a variety of aspects, such as attributes, context, dependencies between actions and participating entities therein.

**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.

**Phase 4: Process implementation** This concerns the effective enactment of GDPR-compliant processes, mainly as regards two aspects. The first entails a comprehensive set of tools able to support the requirements arising from GDPR (data handling, data subjects' involvement, etc.). The second is related to the alignment of modelled processes with the actual infrastructure of the organisation; grounded primarily on the BPR4GDPR semantic foundations, it will enable refinement and adaptation of the models to each organisation's reality.

**Phase 5: Process execution** This extends Phase 4 by ensuring compliant process execution, following the configuration set forth. That is, 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 concerns the use of process mining for process ex post analysis, in order to ensure that specified policies are indeed enforced, fostering accountability. Furthermore, such techniques will enable automatically improving process models over time.

**Phase 7: Common operations** This refers to operations that are not (necessarily) part of a process lifecycle, but are executed asynchronously to processes or are independent thereof. They fall in different categories, including: i) functions that are supportive to all phases (e.g., authorisation mechanisms); ii) enforcement of data subject rights; iii) data management functions; iv) continuous operations, such as risk estimation, 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. In the following, the main principles and technical ideas are summarised.

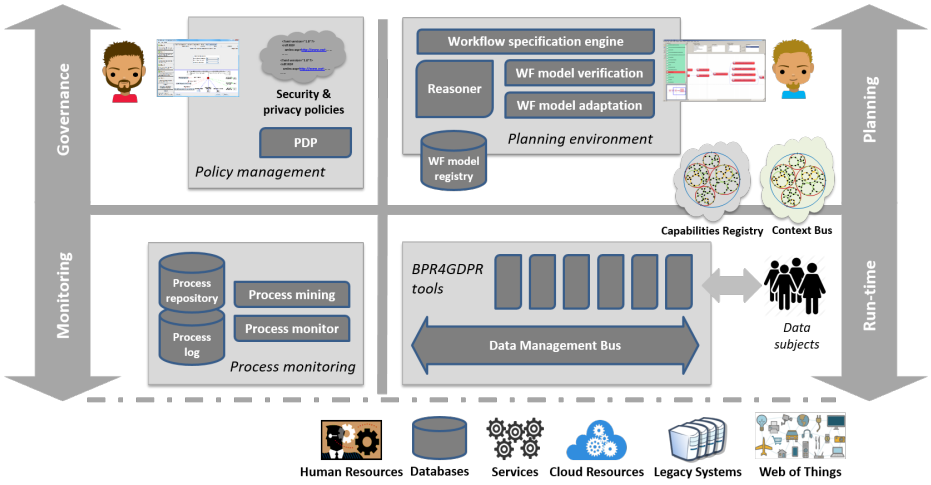


Fig. 2: BPR4GDPR architecture.

**Governance** provides all functions related to policy management, representing the Policy Decision Point (PDP) of the system. In BPR4GDPR, policies hold a dual role: i) they provide the means for system governance, in the sense that they set the rules that regulate the operation of BPR4GDPR components; ii) they comprise the knowledge base that feeds the procedure of process re-engineering, towards *by design* compliant process models.

To this end, BPR4GDPR develops 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 [8], along with the respective software prototype, whereas policies are grounded on the Compliance Ontology, providing a high-level codification of GDPR into concepts that need to be taken into consideration by the policy framework.

**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*. The first step in this direction is facilitated by tools allowing their description in a way that effectively guides their execution, while also being expressive enough to capture associated provisions; these tools are grounded upon prior academic work of BPR4GDPR researchers [7]. Further, in order to automatically incorporate policies as part of workflow design, the BPR4GDPR approach involves sophisticated means for the evaluation of process specifications against a number of compliance aspects. Their main aim is to control access to, usage of, and flow of information and prevent illegitimate activity, as well as to determine whether critical tasks are properly included and, if not, impose their execution.

**Monitoring** deals with process mining and monitoring with the aim to identify discrepancies between compliant and actual behaviour. To this end, BPR4GDPR implements a Privacy-Aware Process Mining Framework, based on mature technology brought by its partners, particularly ProM[2] [2][6]. The approach is primarily based on two concepts: *streaming process mining* [5], that allows analysing real-time data in order to detect problems, anomalies and potential frauds; the *concept drift* issue [4], calling for solutions for change detection and continuous update, in order to handle situations where new factors/requirements render the process model out-of-date and in need to be adapted/improved.

Finally, in order to facilitate the deployment of appropriate technical measures, as required by the GDPR, **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.

In this context, the project provides 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's modules fall into three families:

- Privacy-enhancing technologies, particularly cryptographic tools, devised for data and communications confidentiality, anonymisation and pseudonymisation, as well as enforcement of access rights by cryptographic means ([3]).
- Data management tools that, by means of data access and usage management, provide for controlling data handling, including retention and storage, pre- and post-processing, etc. A core position is held by the Data Management Bus (Fig. 2), comprising the main Policy Enforcement Point (PEP).
- User-centered tools, providing for the enforcement of the data subjects' rights, including information and notification, consent, and consideration of own preferences as regards data handling.

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

## 4 Conclusion

In the rapidly maturing privacy market, currently available solutions do not appear to sufficiently cover important GDPR aspects, while process orientation has not been extensively incorporated either. In order to address such shortcomings, BPR4GDPR aims to offer *privacy-by-design* throughout the entire process lifecycle, based on a broad spectrum of innovations. These will concern, at a first stage, process analysis and redesign, i.e., automatic verification of process models according to GDPR provisions but also transformation of non-conformant ones. Further, a compliance toolkit will be devised encompassing sophisticated functionalities, such as cryptography, data handling and notification mechanisms, as well as user-centered tools ensuring consent, but also the exercise of other data subjects' rights. From another perspective, process mining will be used for process discovery, process monitoring and controlling, enabling a posteriori analysis and compliance check of running processes. BPR4GDPR will thus provide a user-friendly environment for the definition of inherently GDPR-compliant processes and the automatic inclusion of necessary measures, relieving end-users from the considerable operational burden of continuous compliance assessment, and preventing business and other risks associated with potential violations.

## 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 BPM Demos (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. Hassani, M.: Concept drift detection of event streams using an adaptive window. In: ECMS 2019 Proceedings of the 33rd European Council for Modeling and Simulation. (to appear) (Jun 2019)
5. 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)
6. 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 (2014)
7. Koukovini, M.N.: Inherent privacy awareness in service-oriented architectures. Ph.D. thesis, National Technical University of Athens (2014)
8. Papagiannakopoulou, E.I.: Semantic Access Control Model for Distributed Environments. Ph.D. thesis, National Technical University of Athens (2014)