Gap
The Business Process Model and Notation (BPMN) is a standard notation for capturing enterprise-wide and interorganizational business processes. BPMN models are commonly used to analyze the compliance of business processes with respect to regulations [2] as well as their performance with respect to efficiency and quality criteria [3].

A less exploited application of BPMN models is to analyze compliance with respect to privacy regulations, in great part because of BPMN’s inability to capture privacy requirements and privacy-enhanced technologies (PETs), such as secure multiparty computation, differential privacy, and homomorphic encryption. Currently, there is no approach available to analyze the way private data is used (and potentially leaked) along entire business processes in the presence of PETs.

Approach
To address this gap, we have designed an extension of BPMN, namely privacy-enhanced BPMN (PE-BPMN), that allows users to capture private data objects, privacy policies, and PETs alongside the tasks, decisions, and other elements of a business process model [4].

To support the design and analysis of PE-BPMN models, we have developed a tool, namely Pleak [5], that allows users to identify privacy leakages in PE-BPMN models, to quantify the extent of these leakages, to determine which PETs can be used to eliminate or reduce these leakages, and to analyze the trade-offs that these PETs bring along, for example in terms of loss of accuracy of the disclosed data.

Pleak supports the analysis of PE-BPMN models at three levels. The top level (Boolean analysis) tells us whether or not a given output of a process may reveal information about a given input. The middle level (qualitative analysis), goes further by indicating which attributes of (or functions over) a given input data object are potentially leaked by each output, and under what conditions this leakage may occur. The lower level (quantitative analysis) quantifies to what extent a given output leaks information about an input, either in terms of a sensitivity (differential privacy) measure or in terms of the guessing advantage that an attacker gains by having the output. The Boolean level is based on the high-level flow of the data and privacy-enhancing technologies that are deployed to avoid leakages. In the qualitative and quantitative levels, Pleak relies on the specification of the actual computations carried out by the steps in the business process, as well as the definitions of data structures. Quantitative analyses output both the
expected privacy risk and the necessary measures to overcome the leakage. In addition, they highlight the trade-off of a private process versus an accurate process. Furthermore, Pleak can also make use of the actual data used in the process (or data samples) if available.

With respect to previous research proposals on privacy analysis of business processes [1], Pleak stands out for its ability to analyze processes not only in terms of yes-no questions (e.g., is private data unduly disclosed to a given party?) but also in quantitative terms, allowing analysts to address questions such as: How much private information about a given individual can a participant in a process infer from the data disclosed to them? Or, how much noise should be added to the data disclosed to a party so that this party cannot infer some private information within certain bounds?

Pleak has been validated via three case studies in the fields of emergency response, international aid distribution, and IoT-based building occupancy monitoring. The case studies have demonstrated the usefulness of combining qualitative and quantitative analysis to understand the scope and impact of privacy leakages.

An online version of Pleak is available for evaluation purposes at https://pleak.io/. The source code is available at https://github.com/pleak-tools.

References
1. Accorsi R, Lehmann A, Lohmann N (2015) Information Leak Detection in Business Process Models: Theory, application, and tool support. Inf Syst 47: 244–257
2. Governatori G, Milosevic Z, Sadiq S (2006) Compliance checking between business processes and business contracts. In: Proceedings of the 10th International IEEE Enterprise Distributed Object Computing Conference, pp 221–232
3. Van Looy A, Shafagatova A (2016) Business process performance measurement: A structured literature review of indicators, measures and metrics. SpringerPlus 5(1):1797
4. Pullonen P, Tom J, Matulevičius R, Toots A (2019) Privacy-enhanced BPMN: Enabling data privacy analysis in business processes models. Softw Syst Model. https://doi.org/10.1007/s10270-019-00718-z
5. Toots A, Tuuling R, Yerokhin M, Dumas M, García-Bañuelos I, Laud P, Matulevičius R, Pankova A, Pettai M, Pullonen P, Tom J (2019) Business Process Privacy Analysis in Pleak. CoRR abs/1902.05052 (2019). https://arxiv.org/abs/1902.05052