Notice of the Final Oral Examination
for the Degree of Master of Science
of

ZE SHI LI

BSc (University of Victoria, 2018)

“Complying with the GDPR in the Context of Continuous Integration”

Department of Computer Science

Tuesday, March 17, 2020
11:30 A.M
Engineering Computer Science Building
Room 548

Supervisory Committee:
Dr. Neil Ernst, Department of Computer Science, University of Victoria (Co-Supervisor)
Dr. Daniela Damian, Department of Computer Science, UVic (Co-Supervisor)

External Examiner:
Dr. Issa Traore, Department of Electrical and Computer Engineering, UVic

Chair of Oral Examination:
Dr. David Leitch, Department of Chemistry, UVic

Dr. David Capson, Dean, Faculty of Graduate Studies
Abstract
The full enforcement of the General Data Protection Regulation (GDPR) that began on May 25, 2018 forced any organization that collects and/or processes personal data from European Union citizens to comply with a series of stringent and comprehensive privacy regulations. Many software organizations struggled to comply with the entirety of the GDPR’s regulations both leading up and even after the GDPR deadline. Previous studies on the subject of the GDPR have primarily focused on finding implications for users and organizations using surveys or interviews. However, there is a dearth of in-depth studies that investigate compliance practices and compliance challenges in software organizations. In particular, small and medium enterprises are often neglected in these previous studies, despite small and medium enterprises representing the majority of organizations in the EU. Furthermore, organizations that practice continuous integration have largely been ignored in studies on GDPR compliance. Using design science methodology, we conducted an in-depth study over the span of 20 months regarding GDPR compliance practices and challenges in collaboration with a small, startup organization. Our first step helped identify our collaborator’s business problems. Subsequently, we iteratively developed two artifacts to address those business problems: a set of privacy requirements operationalized from GDPR principles, and an automated GDPR tool that tests these GDPR-derived privacy requirements. This design science approach resulted in five implications for research and for practice about ongoing challenges to compliance. For instance, our research reveals that GDPR regulations can be partially operationalized and tested through automated means, which is advantageous for achieving long term compliance. In contrast, more research is needed to create more efficient and effective means to disseminate and manage GDPR knowledge among software developers.