Assistance in risk assessment on Corona-tracking app in Norway

Engagement structure

- **KPMG Norway** has multiple ongoing projects with **Norsk Helsenett** (the Norwegian national provider of e-health solutions). In one of those projects, KPMG delivers information security officers that continuously perform risk assessments on new e-health functionality for the national health platform for citizens Helsenorge.no
- **Folkehelseinstituttet** (FHI, the Norwegian Institute for Public Health) has recently asked Norsk Helsenett to assist in the risk assessment of a mobile app with the intended functionality to track an individual's contacts (based on GPS and Bluetooth) and alert in case of contact with a Covid19-infected person. They aim at min 60% usage in Norway (>3 million people).
- In our role as information security officers for Norsk Helsenett, KPMG is therefore involved in this assessment, together with Norsk Helsenett employees and several other third parties.

Scope and approach

- KPMG assisted in the development of risk scenarios, using the ISF IRAM2 framework and KPMGs proprietary tools and standards for risk assessments, that include:
  - An analysis on threat actors, their capabilities and potential intentions towards the geographical and contact information of all app users.
  - Vulnerabilities in the design, development and operation of the app, the cloud environment where information is being stored (Azure based), web applications, APIs, notification services and underlying infrastructure. Technical assessments were performed by other third parties and the results were taken into account in this assessment.
  - Impact areas in terms of C,I and A, as well as reputation / trust of the solution, health, economic and societal impact categories.
- KPMG assisted in the assessment of likelihood and impact per scenario, as well as the establishment of an uncertainty score per scenario. The uncertainty score indicates a confidence level for the likelihood and impact scores of that scenario. With the solution being developed in a very short timeframe and the assessment taking place while development and documentation is ongoing, only limited information has been made available as a basis for the risk scores, which means that uncertainty also needs to be communicated and accepted.
- KPMG provided recommendations on reduction of risk levels for various scenarios and assisted in reporting of the risk assessment outcomes on behalf of Norsk Helsenett to FHI.
- The client has their own team of privacy lawyers; KPMG did not provide assessments or conclusions on compliance with privacy regulations.

Lessons learned

- Communicating uncertainty on top of likelihood and impact gives an more complete picture of the actual risk. After all, one if the biggest overall risks with such fast-developed solutions is that one has not been able to get a full understanding of all consequences. This uncertainty is important to communicate and get accepted by the governmental body before rollout.
- As it is difficult for the application owner (FHI) to articulate the risk appetite, it is very challenging to provide adequate recommendations on risk reduction and acceptance. Namely, the owner needs to balance the information security and privacy risk of the individuals with health and economic risks of the society as a whole, and is under time pressure. It requires a holistic risk view to then be able to come with adequate measures per individual risk scenario.
- Close collaboration with the Norwegian National Security Authority and the Intelligence Service proves to be of value when assessing risks on the scale of a full nation. Typically, KPMG has a business view and therefore may not always have the understanding of threat pictures that national intelligence services have when it comes to state actor presence and intents.