Diarienummer:
IMY-2026-5444

Datum:
2026-03-30

Use of Trusted Execution Environment

English summary

In the present project, the Swedish Authority for Privacy Protection (IMY), together with the participants, has analysed how trusted execution environments (TEE) can be used to protect information processed outside a vehicle's local computing environment. Within the framework of the project, Volvo Group (Volvo) intends to collect data via cameras and sensors installed in Volvo's trucks. These data will be transferred to and processed in a trusted execution environment. The environment is provided by a mobile network operator as a technical service within its infrastructure.

The transfer and processing in the execution environment are necessary because the vehicles' own computing capacity is limited and insufficient to process all data locally in the vehicle. The processing may include personal data, primarily in the form of video material in which road users appear. The trusted execution environment is established through functionalities provided by Ericsson and CanaryBit.

The purpose of the processing is to enable external data processing, that is, processing that takes place outside the vehicle, with a level of security equivalent to that which would have been maintained if the processing had taken place locally within the vehicle's own systems. The project has in particular highlighted how trusted execution environments can contribute to increased security and control over data in use compared with more traditional solutions, such as conventional cloud services.

The questions examined by IMY in the project are which security measures may be appropriate when using trusted execution environments, whether the GDPR applies to the processing in the project, and what potential role, if any, the provider of a trusted execution environment may have under the GDPR.

Conclusions

Which security measures may be appropriate when using trusted execution environments?

IMY emphasises that trusted execution environments can help reduce the risks associated with external processing of personal data, for example the risk of unauthorised or unintended access. The technology can therefore constitute a safeguard that strengthens the controller's actual control over the security of data in use. Compared with conventional cloud solutions, where trust is to a greater extent based on contractual commitments, trusted execution environments enable technically verifiable control over the environment in which data are processed. Through built-in protection mechanisms, both access to data and which code is allowed to be executed are

Postadress:
Box 8114
104 20 Stockholm

Webbplats:
www.imy.se

E-post:
imy@imy.se

Telefon:
08-657 61 00

controlled, thereby strengthening trust in the provider of the technology. In the present project, particular emphasis has been placed on ensuring that key management and the verifier function for the trusted execution environment are handled by the controller. The verifier function performs attestations of the environment, providing technical evidence that it is secure and running the correct program code.

Is the GDPR applicable to the processing?

IMY assumes that personal data will be processed in the envisaged project, for example when individuals are captured in video recordings from the cameras on Volvo's trucks. IMY assesses that the different steps in the process—from the collection of data to their transfer and processing in the trusted execution environment—typically constitute processing by the controller within the meaning of Article 4(2) of the GDPR. As the data are processed automatically by Volvo, the processing falls within the scope of the GDPR.

What role under the GDPR does the provider of a trusted execution environment have?

According to IMY, there are circumstances in this case that suggest that the mobile network operator, which provides computing power and the technical service for the environment, should not be regarded as either a sole or a joint controller for the processing. In many commercial services offering trusted execution environments or similar cloud-based solutions, the provider is typically considered a processor. In the present project, however, there are circumstances that argue against processor status. Of particular importance is that the verifier function is placed within the controller's sphere of control, as well as the mobile network operator's very limited ability to take measures to comply with obligations as a processor, for example ensuring the protection of data subjects' rights. For such an assessment to be maintained in practice, decisions regarding essential means of the processing—such as safeguards and control over the data processed in the trusted execution environment—must rest with the controller. The controller must also be able to demonstrate that the measures intended to prevent the mobile network operator from accessing the content are effective and work in practice.