IMY. Integritetsskydds myndigheten

Trusted execution environments for connected vehicles

Final report from IMY's data protection innovation sandbox

Reference number
IMY-2026-5444

Date
2026-03-30

Table of content

This report has been automatically translated. If the information in English is different from the Swedish version, the Swedish version applies.

Postal address:
Box 8114
104 20 Stockholm
Website:
www.imy.se
E-mail address:
imy@imy.se
Phone number:
08-657 61 00

Glossary

User	The party that transfers data to, and processes data within, a Trusted Execution Environment. The user owns or exercises control over the data to be processed. In the present project, the user is Volvo Group.
Trusted Execution Environment	A hardware-based, isolated, and cryptographically protected processing environment within a processor, designed to enable the protection of data in use by performing computations in a technically segregated and attestation-controlled environment. The English term for the technology is “Trusted Execution Environment” (TEE).
Participants	CanaryBit, Ericsson and Volvo Group
EDPB	European Data Protection Board
GDPR	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).
IMY	Integritetsskyddsmyndigheten
Attestation function	The party that verifies the integrity of the execution environment through attestation and ensures that only authorised code and approved data are transferred into and processed within the environment. In the present project, Volvo Group intends to exercise control over this function itself.
Provider	The party that provides the technical service and computational resources for the execution environment. In the present project, the provider is intended to be a mobile network operator.

1. Summary

1.1. Use of trusted execution environments

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

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

The purpose of the processing is to enable data processing outside the vehicle while maintaining a level of security equivalent to that which would be achieved if the processing were carried out locally within the vehicle's own systems. In particular, the project has examined how TEEs can enhance the security and control over data in use compared with more traditional solutions, such as conventional cloud services.

Within the scope of the project, IMY has examined what security measures may be appropriate when using TEEs, whether the GDPR applies to the processing activities carried out in the project, and the potential role under the GDPR of a provider of a TEE.

1.2. Conclusions

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

IMY emphasises that TEEs can help mitigate the risks associated with the external processing of personal data, including the risk of unauthorised or accidental access. As such, the technology may constitute a safeguard that strengthens the controller's effective control over the security of data while in use. Compared with conventional cloud-based solutions, where trust relies to a greater extent on contractual arrangements and organisational assurances, TEEs enable technically verifiable control over the environment in which data is processed. Through built-in security mechanisms, TEEs can restrict both access to data and the execution of software within the environment, thereby enhancing confidence in the integrity of the processing environment and the provider of the technology.

In the present project, particular importance has been attached to ensuring that both key management and the attestation function remain under the controller's control. The attestation function performs cryptographic attestations of the execution environment, providing technical evidence that the environment is operating in a trusted state and is executing the intended software code.

Is the GDPR applicable to the processing?

IMY proceeds on the assumption that personal data will be processed in the intended project, for example when individuals are captured in video recordings from cameras

installed in Volvo trucks. IMY considers that the various stages of the process — from the collection of data to its transfer and processing in the TEE — will typically constitute processing of personal data within the meaning of Article 4(2) of the GDPR. As the data is 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 the present project indicating that the mobile network operator, which provides the technical service and computing capacity for the execution environment, should not be regarded as either a sole controller or a joint controller in relation to the processing. In many commercial services offering TEEs or similar cloud-based solutions, the provider would typically be regarded as a processor. In the present project, however, there are circumstances that weigh against such a classification. Of particular significance is the fact that the attestation function remains within the controller's sphere of control. Equally important is the mobile network operator's very limited ability to take measures necessary to fulfil obligations typically associated with the role of a processor, including obligations relating to the protection of data subjects' rights. For such an assessment to be sustained in practice, decisions concerning the essential means of the processing—including the safeguards applied and control over the data processed within the TEE—must remain 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 operate as intended in practice.

2. The project

2.1. Background

In data processing, a distinction is often made between three states of data: in transit, at rest, and in use. Encryption and other similar protective mechanisms are now well established for data that is being transmitted or stored.

In today's digital society, vast amounts of information — often of a sensitive nature — are processed, ranging from specially protected categories of personal data to security settings and location information. As a result, the need to protect information throughout its entire lifecycle has become increasingly important.

While robust protection mechanisms exist for data in transit and data at rest, significant challenges remain with regard to the protection of data in use. In order to be processed, data must typically be accessible in an unencrypted form, which increases its vulnerability to unauthorized access or manipulation. Protecting data in use has therefore become a central and complex issue within modern information security.

One of the technologies developed to address this challenge is the trusted execution environment (TEE). A TEE may be described as a hardware-based, isolated execution environment within a processor, in which information can be processed separately from the rest of the system. Only pre-authorised and approved code is permitted to execute and access the data processed within the environment. In addition, data processed within the TEE remains cryptographically protected from external parties, making it extremely difficult to access, read, or manipulate the content — even in cases involving physical access to the device or access through system interfaces.

2.2. The project goals

The objective of the project is to examine how TEEs can be used to enable secure data processing in situations where the computational capacity of a local device is insufficient. By using TEEs, processing may be carried out by an external party without the mobile network operator providing the computational resources and technical service for the environment gaining access to the data processed within it. This makes it possible for processing to take place outside the local computing environment, using infrastructure provided by an external provider, while maintaining a level of protection comparable to that which would have applied had the data been processed locally within the device itself.

2.3. The project participants

CanaryBit is a company that develops solutions for secure data processing. In this project, CanaryBit provides code used to initialize and run a TEE.

Ericsson is a provider of information and communication technology and, together with CanaryBit, supplies the software and functionalities required to operate the TEE in the project—primarily in the form of software and a controller function.

Volvo Group is a global vehicle manufacturer with a wide range of connected services. Within the scope of this project, the data collected by Volvo's trucks will be transferred and processed in a TEE.

2.4. The technology

A TEE is a protected area within a processor in which program code can be executed and data can be processed within a separate and secure memory space. The environment is isolated from the rest of the system and protected through both hardware-based isolation and cryptographic mechanisms. Its purpose is to safeguard information even in situations where the operating system or other parts of the system may be compromised.

Technically, a TEE is established through dedicated security functionalities embedded in the processor hardware. These functionalities enable specific code and data to be isolated from other parts of the system. Code executed outside the TEE has no access to the information processed within the environment and is therefore unable to read, modify, or manipulate it. In this way, the system is divided into two categories of environments: a normal world, in which the operating system and ordinary applications operate, and one or more secure worlds (isolated execution environments), in which only specifically authorised code is permitted to execute and process protected information.

A central feature of TEEs is attestation. Through attestation, the TEE can generate cryptographic proof of its current state and of the software code executing within the environment. This proof may be used by a dedicated verifier function to confirm that the environment satisfies predefined security requirements before any data is permitted to be processed within it.

In practice, data is transmitted to the TEE in encrypted form and is decrypted only upon entry into the isolated environment in which the processing takes place. Because the protection is enforced at the hardware level — rather than relying solely on the operating system — the information may remain protected even where other parts of the system are compromised or cannot be fully trusted.

2.5. Privacy-enhancing technologies

Privacy-enhancing technologies (PETs) is an umbrella term for technical solutions designed to protect individuals' privacy. From a data protection perspective, PETs can help strengthen the protection of personal data during processing, for example by limiting the exposure of personal data or preventing unnecessary or unauthorised processing of personal data.[1]

TEEs constitute one category of privacy-enhancing technology. The security of these environments is based on a number of security mechanisms inherent in the underlying technical architecture, including isolation, access control, and cryptographic protection. Together, these mechanisms contribute to embedding data protection into the design of the system and may therefore serve as an example of how the principle of data protection by design can be implemented in practice.[2]

The use of TEEs has increased significantly over the past decade and the technology is now used in a wide range of applications, including mobile devices (for the protection of biometric data), payment services, and digital identity solutions.[3] In cloud computing environments, TEEs can enable secure processing of information without the cloud

[1] For further information, see, for example ENISA, Data Protection Engineering – From Theory to Practice, and OECD, Emerging Privacy Enhancing Technologies: Current Regulatory and Policy Approaches.
[2] Article 25.1 GDPR.
[3] European Data Protection Supervisor, Tech Sonar Report 2025–2026, p. 24 ff.

provider gaining access to user data. Secure execution environments are also used in industrial processes, IoT devices, and edge computing systems to establish trust in distributed environments where multiple parties interact without requiring full mutual trust.

2.6. Data protection questions

The project participants, together with the Swedish Authority for Privacy Protection (IMY), agreed to focus on the following data protection issues in the present project:

- What security measures may be appropriate when using trusted execution environments (TEEs)?
- Is the GDPR applicable to the processing?
- What role does the provider of a trusted execution environment have under the GDPR?

2.7. Scope limitations

This report examines the processing of personal data from the point at which the data is collected until it is transmitted to and processed within a TEE. It should be noted that the service under consideration is not yet operational.

The report sets out IMY's legal assessment of those issues for which guidance has been considered necessary. The assessments are based on the legal framework applicable at the time of writing and may need to be revisited in light of future legislative developments, case law, or guidance issued by the EDPB[4].

The guidance provided within the scope of the project is limited to the three data protection issues identified above. In addition to these matters, there are other legal, regulatory, and operational considerations that the participants will need to address before the project can be implemented in practice. Those considerations, however, fall outside the scope of this report.

[4] For further information about the EDPB, please visit IMY's website, https://www.imy.se/verksamhet/dataskydd/dataskydd-pa-eu-niva/edbp/

3. What security measures may be appropriate when using trusted execution environments?

3.1. Security measures and the GDPR

Under Article 32 of the GDPR, controllers and processors are required to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks that the processing poses to the rights and freedoms of natural persons. The provision is based on a risk-based approach and requires consideration of, among other factors, the nature, scope, context, and purposes of the processing, as well as the state of the art. In this context, the use of privacy-enhancing technologies (PETs) may constitute an important means of complying with the requirements of Article 32, as such technologies are designed to minimise the exposure of personal data and reduce the risk of unauthorised access. When properly implemented, PETs can contribute to the protection of personal data throughout its entire lifecycle.

A TEE may itself constitute a particularly relevant technical safeguard, as it enables isolated and protected processing of information, including in environments where the underlying infrastructure cannot be fully trusted.[5] TEEs may be implemented both in local devices and as part of cloud-based services, thereby enabling computations to be performed without requiring the user to manage the underlying hardware infrastructure. TEEs therefore represent one example of a privacy-enhancing technology that can be used to protect data while it is being processed. This section outlines key security considerations relating to the use of TEEs, as well as measures that may be implemented to protect data — including personal data — processed within such environments.

3.2. Security in the use of trusted execution environments

The security of TEEs is based on a number of security mechanisms inherent in the underlying technical architecture. These mechanisms are fundamental to how TEEs are designed and are present to varying degrees in different implementations of the technology. Together, they enable technically verifiable protection of data in use. Below, some of the key mechanisms that generally characterise TEEs are outlined.

3.2.1. Isolation

A key feature of TEEs is technical isolation. This means that data processed within the environment is kept separate from other parts of the system and cannot be accessed by, for example, service providers supplying the underlying infrastructure. During transmission, data is encrypted and is only decrypted within the isolated environment at the point of processing. The combination of isolation and encryption ensures that data is protected both in transit and during processing. From a data protection perspective, this enhances confidentiality and reduces the risk of unauthorised access, even if the surrounding infrastructure is compromised.

[5] See Section 2.4. For further reading, see also, for example, ANSSI, Technical Position Paper on Confidential Computing, p. 2 ff., and EDPS, TechSonar Report 2025–2026, p. 24 ff.

3.2.2. Attestation

For a user to trust that the environment provides the intended protection, verifiability is essential. This requires the ability to verify that processing takes place within a genuine TEE, that the correct software is being executed, and that the environment has not been tampered with or otherwise compromised. The verifiability provided by TEEs is achieved through attestation.

Attestation is a technical and cryptographic process in which the execution environment generates evidence of its current state. This evidence may include information about the code being executed, the security configuration in place, and whether the environment is in a trusted and unaltered state. The attestation output can then be verified by a dedicated validation function, which checks whether the environment meets predefined conditions before any data is permitted to be processed.

Unlike traditional cloud services, where security largely relies on contractual arrangements, policies, and the provider's assurances, attestation provides technical evidence that the environment is in the intended state. This is particularly important where the execution environment is operated by a third party and the user does not have direct physical control over the underlying hardware and infrastructure.

3.2.3. Ephemeral and state-dependent environment

A central, though often less visible, security feature of TEEs is their ephemeral and strictly state-dependent nature. This means that the environment only exists as long as it remains in a state where the correct program code is running, where this can be cryptographically verified, and where only authorized components have access to the environment. If this state is compromised—for example, if unauthorized code is attempted to be executed or if underlying security requirements are no longer met—the environment ceases to exist immediately. Upon such a shutdown, all information within the environment is erased, and no data leaves the environment in plaintext.

This mechanism can be likened to a self-destructing safe. As long as the correct combination is used and no tampering is detected, the contents remain accessible. However, at the slightest deviation in the environment's configuration or codebase, attestation fails, the "safe" stops functioning, and its contents are destroyed.

From a privacy and security perspective, this is particularly significant. In traditional systems, a breach may allow an attacker to gradually map the system, read memory, or analyse processes over time. In a TEE, both the attack surface is more limited and the window of opportunity for exploitation is significantly narrower, as the environment is designed to terminate under unverifiable conditions.

In summary, several of the security features that characterize a TEE enable data to be processed in a more controlled and technically verifiable manner compared to, for example, traditional cloud environments. However, the technology's contribution to security also depends on how it is integrated and configured in the specific processing context.

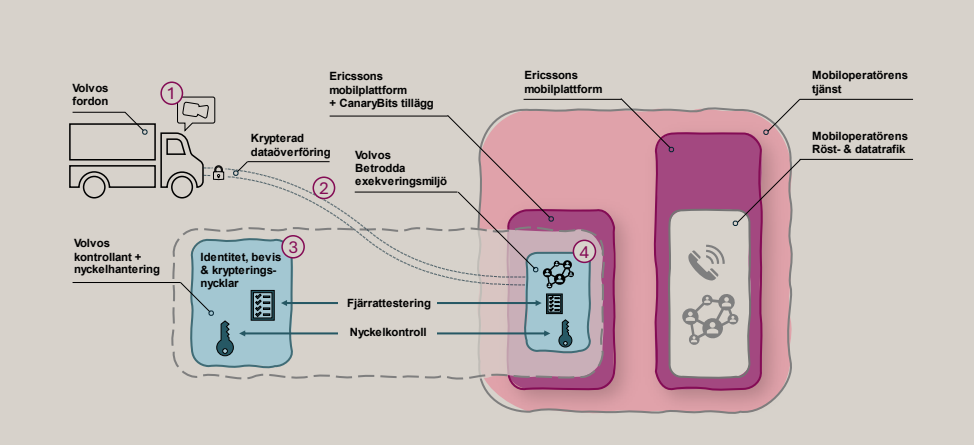
3.3. Implementation of the technology in the present project

In the project, data generated by Volvo vehicles is processed within TEEs. A separate and unique execution environment is established for each truck and remains active only

for as long as the predefined conditions governing the environment are fulfilled. The mobile network operator is intended to provide the technical service and computing capacity required to host the TEE. CanaryBit and Ericsson are responsible for providing the functionalities necessary to establish and operate the environment, primarily in the form of software and an attestation function.

All data processed within the TEE is encrypted during transmission to the execution environment and is decrypted only within the environment itself. As a result, the mobile network operator providing the TEE service neither has, nor is technically capable of obtaining, access to the content processed within the environment.

In summary, the intended use of the TEE within the project is as follows:



1. Volvo transmits data for processing, including video streams and positioning data generated by the truck's cameras and sensors.

2. The data is transmitted over the mobile network through an encrypted connection to a TEE uniquely established for each vehicle. A mobile network operator provides the technical service and computational resources required for the TEE, which forms part of the mobile platform delivered by Ericsson and CanaryBit.

3. Before data can be transferred to and processed in the TEE, predefined security conditions must be satisfied. Through cryptographic key management, the identity and authorisation of the truck's environment are first verified. The trusted and unaltered state of the TEE is then confirmed through attestation. The verification function ensures that only authorised code and approved data are permitted to execute and be processed within the environment.

4. Only after these verification steps have been successfully completed are may the transmitted data be decrypted and processed within the TEE. Data processed in the environment is protected from all other functions in the operating system and surrounding software.

   When data no longer needs to be processed within the TEE, the environment is shut down and dissolved. The TEE is also immediately terminated if the attestation process fails to satisfy the predefined conditions verified by the attestation function.

The implementation examined within the project differs from more conventional commercial implementations of TEEs in two particularly significant respects: the introduction of a self-managed verification function and key management that remains entirely under the control of the user of the environment. These aspects have also been of particular importance to IMY in its assessment of the legal issues arising within the project.

3.3.1. Self-managed or independent attestation function

A key distinction between the implementation examined in the project and many generic cloud-based implementations of TEEs is the introduction of a self-managed attestation function responsible for verifying the integrity of the execution environment. In conventional cloud architectures, the cloud provider commonly acts both as the owner of the infrastructure and as the entity responsible for issuing attestations. As a result, users of the environment must largely rely on the provider's own assurances and security guarantees. The function responsible for verifying the state of the environment is therefore neither organisationally nor functionally independent from the actor operating the infrastructure.

In the present project, control is to a greater extent placed in the hands of the user of the TEE. Volvo governs and is responsible for the attestation function by defining the requirements that must be satisfied for an attestation to be considered valid, including which components are to be verified, which software code may be executed within the environment, and which security configurations are required. Under this model, the mobile network operator merely provides the underlying infrastructure — such as hardware, computational capacity, and network resources — but has no ability to independently approve, control, or influence the attestation of the execution environment.

The attestation function could also be organised through an independent third party providing the technical attestation functionality. Such a solution could further strengthen the independence of the function and contribute to a clearer separation between the actor providing the infrastructure and the actor responsible for verifying that processing takes place within a TEE.

Before data is sealed and processed, the attestation function performs cryptographic attestations of the TEE, thereby providing technical evidence that the environment is secure and running the intended software code. The frequency of attestations plays an important role in determining the level of security. The more frequently attestations are performed, the more rapidly any deviations affecting the integrity of the system can be detected.

Through the self-managed attestation function implemented in the project, potential conflicts of interest are significantly reduced, since no single actor can compromise the platform without such actions becoming detectable through the attestation process. In this way, the user of the TEE does not need to rely solely on contractual arrangements or provider assurances, but can instead use the attestation function to verify the integrity of the entire hardware and software chain.

3.3.2. Key management

In traditional cloud services, cryptographic keys are often managed either by the cloud provider or by the user, which may create vulnerabilities if the keys are exposed or if the

provider has the technical capability to access them. The solution implemented in the project instead applies a model in which the user retains control over the root keys by ensuring that cryptographic keys are released into the execution environment only following successful attestation. In addition, the keys are cryptographically bound to the specific state of the execution environment, preventing their use in an environment that has been compromised or incorrectly configured. This model therefore minimises the risk of key leakage and helps ensure that the user retains effective control over the data processed within the environment.

3.3.3. IMY's comments

Against the background of the above, the use of TEEs may constitute a technical safeguard that strengthens the controller's effective control over the security of data while in use. Compared with conventional cloud solutions, where trust largely depends on contractual arrangements and provider assurances, TEEs enable technically verifiable control over the environment in which data is actually processed.

A central component in achieving such control is the possibility of technical verification through attestation. In the present project, this verification is carried out through a self-managed attestation function that continuously assesses the state of the execution environment and ensures compliance with predefined security requirements. If the environment is manipulated or otherwise deviates from these requirements, the data remains encrypted and the execution environment is terminated. As a result, processing can only take place when the technical preconditions for the processing are satisfied. This not only strengthens security from a technical perspective, but also supports the controller's ability to demonstrate that the processing takes place under controlled and verifiable conditions.

In this context, key management is of particular importance for maintaining effective control over the processing. Where the controller retains control over the encryption keys, or entrusts their management to an independent trusted third party, control over access to the data is significantly strengthened. In the present project, the encryption keys are managed not by the mobile network operator providing the technical service and computational resources for the execution environment, but by Volvo. This reduces the risk of the mobile network operator gaining access to the data processed within the environment.

Overall, TEEs may contribute to reducing the risks associated with external processing of personal data, in particular the risk of unauthorised access to data. This is especially relevant where the infrastructure supporting the environment is provided by an external actor, such as the mobile network operator in the present project. By technically controlling who may access the data and which code may be executed, reliance on the provider can be supplemented by safeguards embedded directly into the technical architecture. In this way, security does not depend solely on organisational commitments, but also on verifiable technical protections.

In the longer term, this may enable new forms of data sharing, as well as analysis and cooperation between organisations in situations where privacy risks have previously limited the ability to make use of data. As the technology matures, becomes standardised, and is integrated into an increasing number of hardware platforms, there are therefore strong reasons to expect that TEEs will increasingly be used as a means of protecting data while in use.

At the same time, there are reasons to adopt a nuanced view of the level of protection offered by the technology. TEEs do not provide protection against all types of threats. Research has shown that certain forms of attack — such as side-channel attacks or other advanced attacks targeting hardware or specific implementations — may in some cases circumvent the protection mechanisms provided by the environment. In addition, the hardware manufacturer itself constitutes the root of trust in this model, since it is the manufacturer that develops and provides the software and mechanisms intended to guarantee the confidentiality and integrity of data within the execution environment. Trust in the technology therefore also depends on trust in the supply chain, which raises questions relating to certification, auditing, and transparency concerning how the technology is developed and implemented.

The use of TEEs therefore does not in itself guarantee compliance with data protection legislation. The actual level of security and privacy protection depends to a large extent on how the technology is implemented and used in practice. Vulnerabilities in application code, deficiencies in configuration, or unclear allocation of responsibilities between actors may in some cases undermine the protections the technology is intended to provide. From this perspective, TEEs should not be regarded as a universal solution, but rather as a complement to other technical and organisational safeguards.

4. Is the GDPR applicable to the processing?

4.1. Processing under the GDPR

The applicability of the GDPR in the project requires, first, that the data in question constitutes personal data and, second, that the activities carried out it involve processing within the meaning of the GDPR.

4.1.1. Personal data

Personal data is defined in Article 4(1) of the GDPR as any information relating to an identified or identifiable natural person. Recital 26 of the GDPR states that, in assessing whether a person is identifiable, account should be taken of all the means reasonably likely to be used, either by the controller or by another person, to identify the individual, considering factors such as the costs involved, the time required, and available technology. Information that cannot be linked to an identified or identifiable natural person by such means does not constitute personal data.

Whether a person is identifiable must be assessed on a case-by-case basis and in light if the actual capabilities of the controller. Consequently, the same set of information may constitute personal data for one controller that has reasonable means to identify an individual, while the assessment may differ for another controller who is effectively shielded from such possibilities.[6]

4.1.2. Processing

Where data constitutes personal data at a given stage, the next step is to determine whether the operations carried out at that stage amount to "processing" within the meaning of Article 4(2) of the GDPR.[7] The concept of processing is intended to be interpreted broadly and in a technology-neutral manner.[8] It encompasses any operation or set of operations performed on personal data, whether by automated means or otherwise.[9] The substantive provisions of the GDPR generally apply to processing activities, including both the collection of personal data and subsequent operations involving the same data, such as storage and transmission.[10]

4.1.3. IMY's comments

Within the project, data is collected, for example, through video recordings captured by the truck's cameras. Volvo has stated that such recordings may contain information relating to identifiable individuals. Before data transferred from the vehicle may be decrypted and processed within a TEE, it is verified through an attestation function.

Against this background, IMY considers that Volvo's handling of personal data constitutes processing during the collection of the data, as well as during its transmission to and processing within the TEE, insofar as the data processed constitutes personal

---

[6] For further information on the concept of personal data, see the judgments of the Court of Justice of the European Union in European Data Protection Supervisor v Single Resolution Board, Case C-413/23 P, EU:C:2025:645, and Gesamtverband Autoteile-Handel, Case C-319/22, EU:C:2023:837.
[7] CJEU, Fashion ID, C-40/17, EU:C:2019:629, p. 71–72.
[8] See Recital 15 GDPR.
[9] Such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.
[10] Westman, D. Dataskyddsförordningen, Artikel 4.2, Karnov 2026-03-24 (JUNO).

data. Since the processing involves personal data processed by automated means, the GDPR applies to all stages of the processing chain that Volvo intends to carry out within the scope of the project.

This assessment is also relevant for the subsequent analysis of the role of the mobile network operator as the provider of the TEE.

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

5.1. Roles under the GDPR

Determining the roles of the various actors involved in, or otherwise connected to, the processing of personal data is essential from a data protection perspective. The allocation of roles determines the responsibilities of the actors under the GDPR and clarifies how data subjects may exercise their rights. The concepts of controller, joint controller, and processor are functional in nature and must be assessed in light of the factual circumstances of the specific processing operation.[11] For the purposes of this project, the term provider refers to the mobile network operator that supplies the technical service and computational resources required for the execution environment.

5.2. Is the provider controller or joint controller?

5.2.1. Controller

Under Article 4(7) of the GDPR, a controller is the natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. In its Guidelines 07/2020 on the concepts of controller and processor, the EDPB emphasises that actual access to personal data is not, in itself, decisive when assessing whether an actor is a controller. Rather, the key consideration is whether the actor exercises genuine influence over the purposes of the processing and the essential means of the processing.[12]

5.2.2. Joint controller

Under Article 26(1) of the GDPR, two or more actors are considered joint controllers where they jointly determine the purposes and means of a particular processing activity. The mere use of shared infrastructure, or the existence of a shared commercial or economic interest, is generally not sufficient in itself to establish joint controllership.[13] The Court of Justice of the European Union (CJEU) has further clarified that joint controllership does not require each joint controller to have access to the personal data being processed.[14]

The CJEU has also confirmed that the absence of direct access to personal data does not, in itself, preclude an actor from being regarded as a controller or joint controller. An actor may still be classified as a controller where it exercises genuine influence over the purposes and essential means of the relevant processing activity, even if it does not have direct access to the data itself.[15]

5.2.3. IMY's comments

In the present project, Volvo alone determines the purposes of the processing and the essential means by which it is carried out. The mobile network operator does not participate in decisions concerning which data is processed, for what purposes the

[11] EDPB Guidelines 07/2020, p. 10, para. 12.
[12] EDPB Guidelines 07/2020, p. 19, para. 45.
[13] EDPB Guidelines 07/2020, p. 23, para. 68.
[14] CJEU, Fashion ID, C-40/17, EU:C:2019:629, p. 69.
[15] CJEU, IAB Europé, C-604/22, EU:C:2024:214, p. 69.

processing takes place, or under what conditions it may be carried out. Nor does the mobile network operator administer the attestation function or exercise any control over the encryption keys or the software permitted to execute within the environment. In these circumstances, there is little to indicate that the mobile network operator participates in determining either the purposes or the essential means of the processing.

Against this background, IMY considers that the circumstances of the project indicate that the mobile network operator, in its capacity as the provider of the TEE, should not be regarded as either a controller or a joint controller in relation to the processing carried out within the TEE.

5.3. Is the provider a processor?

5.3.1. Processor

Under Article 4(8) of the GDPR, a processor is a natural or legal person, public authority, agency, or other body that processes personal data on behalf of a controller. For an actor to qualify as a processor, two conditions must be met. First, the actor must be a separate legal entity from the controller. Second, the actor must process personal data on the controller's behalf and within the framework of the controller's purposes and instructions.[16]

A defining characteristic of the role of a processor is that the processor carries out processing activities on behalf of the controller[17] or is entrusted with performing such activities.[18] In other words, the processor processes personal data under the controller's instructions, while operating outside the controller's direct organisational control. This separation of control gives rise to a potential risk that the protection of data subjects' rights and freedoms may be weaker than if the processing were carried out directly by the controller.

To address this risk and ensure compliance with the GDPR, processors are subject to a number of independent obligations, particularly in relation to the security of processing.[19] Correspondingly, controllers are required to engage only those processors that provide sufficient guarantees that appropriate technical and organisational measures will be implemented in a manner that ensures compliance with the GDPR and safeguards the rights of data subjects.[20] The relationship between the controller and the processor must also be governed by a contract or other legally binding act, commonly referred to as a data processing agreement.[21]

A processor must assist the controller, through appropriate technical and organisational measures, in fulfilling the controller's obligations under the GDPR, including those relating to the rights of data subjects. Upon completion of the processing, the processor must, in accordance with the controller's instructions, delete or return all personal data unless otherwise required by law. However, not every service provider that processes personal data in some manner while delivering a service should be regarded as a processor. The concept of a processor presupposes that the provider actually performs

[16] EDPB Guidelines 07/2020, p. 28, para. 76.
[17] See Recitals 79 and 81 GDPR.
[18] See Recital 81 GDPR.
[19] See Article 28.3 GDPR.
[20] See Article 28.1 GDPR.
[21] Article 28.3 GDPR.

processing activities that form part of the controller's processing operations and does so on behalf of the controller.[22]

5.3.2. Examples of relationships

In its guidelines, the EDPB provides several examples of service relationships that may assist in assessing the role of the mobile network operator as the provider of the TEE in the present case.

- *Hosting services*
  An internet service provider offering a hosting service is generally regarded as a processor in relation to the data stored by its customer on the hosted server, even where the data is encrypted.[23] Hosting services often indicate a processor role where the provider offers a continuous storage service as part of the customer's processing chain, even where the data is encrypted.

  Hosting services typically indicate a processor relationship where the provider delivers an ongoing storage service that forms a part of the customer's processing operations, regardless of whether the provider has practical access to the content of the data.

- *IT consultant engaged fixing a software bug*
  An IT consultant engaged by a company to remedy a software defect may require system access that enables access to personal data. Whether the consultant act as a processor depends on the nature of the assignment, the activities actually performed, and whether any processing of personal data is earned out on behalf of the controller.[24]

- *Cleaning services*
  A cleaning company engaged by a business is not normally intended to process personal data. Where the business has implemented appropriate security measures to prevent access to personal data, the cleaning company and its employees may be regarded as third parties rather than processors.[25]

The examples above illustrate that the assessment of an actor's role must be made based on the activities the actor actually performs and the function it fulfils within the overall processing operation. One relevant consideration is whether the processing of personal data forms an integral part of the service provider that the controller has entrusted to the actor.[26] Another important consideration is that the mere possibility of the temporary access to personal data does not, in itself, determine the actor's role. Such access must instead be assessed in the light of the nature of the assignment, the practical arrangements governing access, and the actor's degree of influence over the essential means of the processing.[27]

5.3.3. IMY's comments

Against the background of the above, it is clear that, in the present project, the mobile network operator constitutes a separate legal entity from the controller, namely Volvo.

[22] EDPB Guidelines 07/2020, p. 29, para. 82.
[23] EDPB Guidelines 07/2020, p. 16, see the example "Hosting services".
[24] EDPB Guidelines 07/2020, p. 28, see the example "IT consultant fixing a software bug".
[25] EDPB Guidelines 07/2020, p. 29, see the example "Cleaning services".
[26] See Recital 81 of the GDPR, which refers to entrusting processing to a processor.
[27] EDPB Guidelines 07/2020, p. 28, see the example "IT consultant fixing a software bug".

The central question is therefore whether the mobile network operator can be regarded as processing personal data on behalf of Volvo and in accordance with Volvo's instructions.

This assessment does not affect the mobile network operator's responsibility for its own processing activities. For example, the operator may act as a controller in relation to traffic data, customer data, and other processing operations carried out pursuant to the Act (2022:482) on Electronic Communications.[28]

TEEs have gained increasing prominence in recent years in response to the growing need for secure mechanisms to protect data while in use. At the same time, guidance concerning the allocation of roles and responsibilities in such environments remains limited. The assessment of roles under data protection law—and, in particular, whether a provider of a TEE should be regarded as a processor—must therefore be based on established principles and general practice. The assessment should focus on the activities actually performed by the actor, as well as the degree of influence exercised over the purposes and essential means of the processing.

The EU legislator's decision to impose specific obligations on processors is closely linked to their practical ability to contribute to the protection of data subjects' rights and freedoms.[29] It is therefore important to consider both the actor's actual capacity to provide such protection and the extent to which it is reasonable to impose processor obligations in light of the nature of the services provided.

In this context, situations may arise in which an actor is neither a controller nor a processor. This may be the case where the actor has been engaged to perform a task that is not intended to involve the processing of personal data and where such processing does not form part of the actor's core responsibilities. Examples include situations in which the actor has no access to personal data, or where any access is merely incidental, highly restricted, or temporary and is not necessary for the performance of the assignment.

Furthermore, the actor may be contractually prohibited from processing personal data except as expressly authorised. In such circumstances, however, the controller remains responsible for ensuring that appropriate safeguards are in place in accordance with Article 32 GDPR, including confidentiality obligations and other technical and organisational measures designed to prevent unauthorised or accidental access to personal data.

5.3.4. The significance of the attestation function in the assessment of processor status

The attestation function described in Section 3.3 is of particular relevance when assessing the role of the mobile network operator. The function is responsible for verifying the integrity of the TEE and for managing the authorisations and cryptographic keys required for processing to take place within the environment.

In the present project, the attestation function enables Volvo to determine which software may be executed within the TEE and under what conditions processing may occur. The function is also designed to suspend and terminate the execution environment if the predefined conditions for processing are no longer satisfied. As a

[28] See for example Act (2022:482) on Electronic Communications, chapter 9.
[29] See for example Article 28.3 c GDPR.

result, the actor controlling the attestation function exercises significant influence over essential aspects of the processing, including control over access to the data processed within the TEE.[30]

Another factor that may be relevant to the assessment is the transient nature of the execution environment. The TEE is instantiated following successful attestation and is dismantled once processing has been completed or the conditions for continued operation are no longer met. Unlike traditional cloud or hosting services, the TEE does not function as a persistent environment for the storage of data at rest.[31]

This architectural design may be relevant when assessing whether the provider merely supplies infrastructure and computing resources or whether it performs processing activities on behalf of the controller. The fact that the environment is created, controlled, and terminated through mechanisms governed by the controller may therefore be a factor weighing against characterising the provider as a processor, although the assessment must ultimately be based on the specific circumstances of the processing in question.

5.3.5. Other relevant factors

In many commercial service offerings involving TEE or similar cloud-based solutions, the provider will typically be regarded as a processor. This is primarily because the provider supplies execution and/or storage services that form part of the controller's processing operations, often including functions such as support, maintenance, and incident management. In such circumstances, the provider will generally be considered to process personal data on behalf of the controller.

The solution examined in the present project, however, differs in several significant respects from these more conventional service models. The TEE has been designed and implemented in a manner that prevents the mobile network operator from accessing the content processed within the environment. At the same time, responsibility for attestation, key management, and access control remains entirely within the controller's sphere of control.

Against this background, and having regard to the purpose of the processor role and the characteristics that define it under the GDPR, a number of factors may be relevant when assessing whether the provider of the execution environment should be regarded as a processor. Where these factors are present in the processing carried out within the TEE, they may weigh significantly in the assessment and, depending on the circumstances, may be decisive in determining whether the provider is acting as a processor.

- The attestation function (including attestation, access control, and key management) remains entirely within the controller's sphere of control and is not administered by the external provider of the TEE.
- The TEE is established on a temporary basis and only operates while predefined conditions are satisfied. Once those conditions are no longer met, the environment is automatically terminated. Unlike a storage service, the processing is therefore not continuous in nature. Consequently, there is no

[30] EDPB states that the essential means include, inter alia, the ability to determine which persons are authorised to access the data.
[31] Cf. the EDPB example "Hosting service", in which the service provider is considered a processor because the data is stored with the service provider.

personal data remaining within the environment that must be returned or deleted once the service has ended.

- The provider's role is limited to supplying infrastructure and computing resources and does not extend to administering the attestation function or exercising control over what is executed within the TEE.
- The provider has no technical ability to access the content processed within the execution environment, as it does not possess the encryption keys, lacks access to relevant technical interfaces, and has no organisational procedures enabling content-level access or processing.
- The provider lacks practical ability to assist the controller and fulfil obligations typically associated with the processor role, including obligations relating to the protection of data subjects' rights.
- The controller is able to demonstrate that appropriate security measures are maintained within the TEE without issuing processing instructions to the provider, reflecting the fact that the provider lacks the practical ability to influence or control the processing carried out within the environment.

5.3.6. Overall assessment

A natural starting point is to regard a provider of a service involving the processing of personal data as a processor. This approach is supported by established practice relating to cloud services and similar arrangements, where the service provider is typically considered to process personal data on behalf of the controller. In that respect, there are factors in the present case that could support the view that the operator providing the TEE acts as a processor.

However, the circumstances of the present project also point towards a different conclusion. Of particular significance is the fact that the attestation function remains under the controller's control. As a result, the mobile network operator has no technical ability to access the data processed within the environment or to influence the processing itself. Similarly, the encryption keys remain entirely under the controller's control. Another factor weighing against the classification of the mobile network operator as a processor is its very limited ability to assist the controller in fulfilling obligations under the GDPR, including obligations relating to the protection of data subjects' rights and freedoms. Responsibility for the fundamental decisions concerning safeguards and control over the processing rests with the controller, who must also be able to demonstrate that the measures designed to prevent access by the mobile network operator are effective in practice.

Taken together, these circumstances may weigh against the conclusion that the mobile network operator processes personal data on behalf of the controller and therefore acts as a processor in relation to the processing carried out within the TEE.

At the same time, the assessment of roles must ultimately be based on the processing activities that actually take place in connection with the operation of the service. It is therefore necessary to examine whether the provider's role is limited to supplying infrastructure and computing resources, or whether the provider, through the operation and administration of the service, performs processing activities involving personal data on behalf of the controller. In a situation where the provider lacks any practical ability to influence the processing, there may likewise be no meaningful need for the controller to issue instructions concerning the processing, since the provider would be unable to act upon them.

If, in the particular circumstances of the case, the provider's role is in practice confined to supplying infrastructure and computing capacity, without performing processing activities on behalf of the controller, this may weigh against classifying the mobile network operator as a processor. The assessment may also be influenced by the contractual terms governing the service, together with the way in which the infrastructure is designed, operated, and used in practice.

The decisive consideration is therefore whether the circumstances described above are reflected in the actual operation and management of the service. If the provider is effectively prevented from accessing the content processed within the environment, lacks technical access paths even for support and incident-management purposes, and does not administer the attestation function, these factors collectively weigh against the conclusion that the provider processes personal data on behalf of the controller and, consequently, against classifying the provider as a processor.

6. Other reflections

Finally, IMY would like to highlight the positive contribution that privacy-enhancing technologies can make to the field of data protection. When appropriately designed, implemented, and integrated into processing operations, such technologies can help mitigate privacy risks, strengthen the protection of personal data, and facilitate compliance with the principles of data protection by design and by default, as well as the obligation to implement appropriate technical and organisational measures to ensure the security of processing.

IMY therefore welcomes initiatives aimed at exploring, testing, and advancing the use of privacy-enhancing technologies. One current example is the forthcoming governmental inquiry into privacy-preserving methods for a more data-driven and collaborative public administration.[32] The purpose of the inquiry is to examine the legal and practical conditions necessary to enable more effective information sharing through the use of, among other things, privacy-enhancing technologies. In IMY's view, privacy-enhancing technologies have the potential to serve as an important tool for reconciling a high level of protection for personal privacy with the need for organisational development, innovation, and more effective use of data. IMY considers this balance to be both necessary and desirable in order to support continued digitalisation while maintaining a strong framework for the protection of fundamental rights and freedoms.

[32] Dir. 2025:64, Integritetsbevarande metoder för en mer datadriven och samverkande förvaltning.

7. Further exploration

This section contains examples of materials referenced in the report that may be of interest for further reading and deeper study.

For guidance on the roles of controller, joint controllers, and processors, as well as the distinction between them, reference is made to EDPB's Guidelines 07/2020 on the concepts of controller and processor in the GDPR.

For further reading on privacy enhancing technologies and trusted execution environments, see for example ENISA, Data Protection Engineering – From Theory to Practice och OECD, Emerging Privacy Enhancing Technologies: Current Regulatrory and Policy Approaches.

For further reading on use cases for trusted execution environments, see for example EDPS, TechSonar Report 2025–2026.

Below is a list of final reports from projects conducted within IMY's innovation sandbox. The references are intended for further reading and deeper study beyond the scope of this report. For an up-to-date overview of published sandbox reports, see IMY's website.

Published reports:

- Federerad maskininlärning mellan två vårdgivare, 15 mars 2023 (IMY-2023-2602).
- Trygghetsmätning i offentliga miljöer med hjälp av IoT-teknik, 9 februari 2024 (IMY-2023-15495).
- Utlämnande av allmänna handlingar med hjälp av AI, 7 november 2024 (IMY-2024-5156).
- Delning av kunduppgifter mellan banker i syfte att motverka ekonomisk brottslighet, 19 maj 2025 (IMY-2024-14275).
- Vidarebehandling av personuppgifter i vårdnadsärenden för att träna en AI-modell, 9 december 2025 (IMY-2025-23536).