Graf von Westphalen

23 November 2022

Moove Connected Mobility B.V.

Data Privacy and IT-Security Compliance

Dr. Michael Herold, M.C.L. Lawyer, Data Protection Officer (TÜV),
Associated Partner

moove®
people. fleet. impact.

Whitepaper

A. Purpose of this document

Compliance with the highest data protection and IT security standards is of central importance to Moove Connected Mobility B.V ('Moove'), to your company and employees and to all other individuals.

We see and understand that privacy may put some people in doubt about telematics services. In this paper we explain to you how Moove complies with the highest data protection and IT security standards to protect the privacy of each individual we work with.

Moove does not only comply with currently applicable data protection and IT security standards and regulations but is also constantly monitoring, updating and advancing in terms of data protection and IT security, especially with regard to changes in the legal situation, even beyond what is required by law.

B. In collaboration with GvW Graf von Westphalen

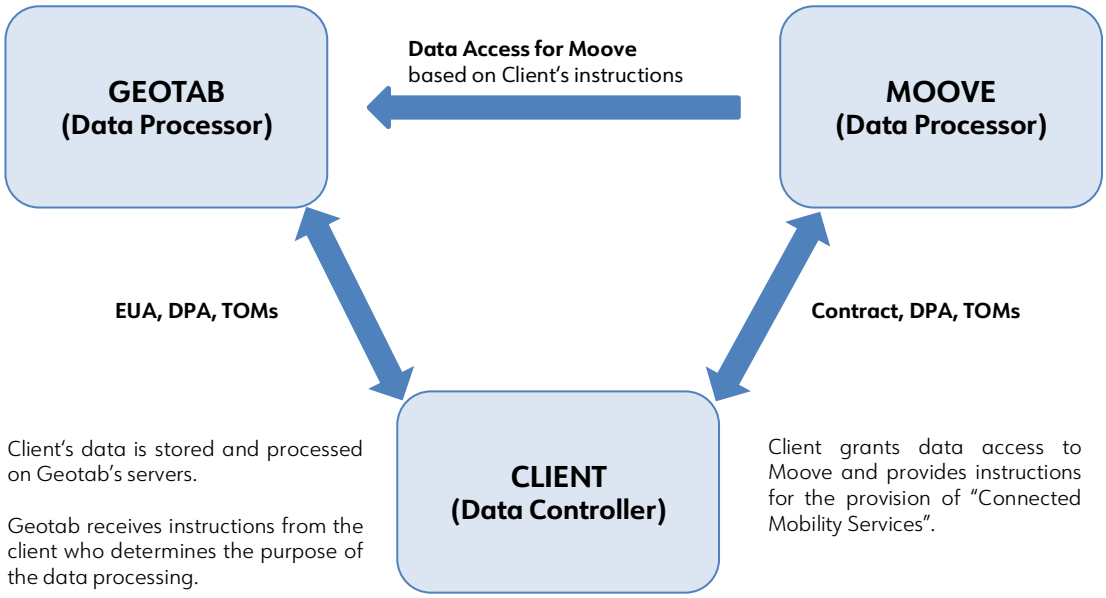
This paper is created in collaboration with GvW Graf von Westphalen (GvW). GvW is a general partnership of attorneys and tax advisors with more than 200 legal professionals. It is one of Germany's largest independent law firms. One of GvW's areas of expertise is digitalization and technology including data protection and IT security. Especially mobility and digital networking are increasingly having an impact on day-to-day business and working life. Understanding, applying and shaping the legal environment in this process is the focus of GvW's advice in this area, which they offer with many years of cross-sector experience and seasoned expertise in all major legal fields. GvW has done a deep dive in all the processes of Moove and approves this paper.

C. The Moove business model in a nutshell – fleet telematics

In cooperation with Geotab Inc. ("Geotab"), a company with head office in Oakville, Ontario, Canada and affiliates and offices worldwide, also in Germany (Geotab GmbH, 52134 Herzogenrath, for more information see geotab.com), Moove offers access to a wide range of telematics data. Such data comes from the engine management (on board diagnostics) and from additional devices and sensors (internet of things). Based on this M2M generated data, which Moove provides to its clients via

customised interfaces and dashboards, referred to as the "Connected Mobility Services", Moove enables its clients to adjust their business operations and thus improve road safety, carry out vehicle maintenance more efficiently and/or reduce the burden on the environment.

Data Processing Relationships



D. Data Privacy

1. Basics

For comprehensive information on data privacy at Moove, please refer to the Privacy Policy available under http://mooveconnectedmobility.com/privacy-policy.

2. Organisation

2.1 Employees

Moove ensures compliance with highest possible data protection and data security through providing comprehensive information and regular training as well as through strict obligations of the employees to data secrecy and confidentiality.

2.2 Privacy Officer

Moove has appointed an (external) Privacy Officer to ensure that the rights of the data subjects under the applicable data protection laws and regulations (GDPR and BDSG) are protected.

The Privacy Officer can be contacted directly at angelika@compleye.io.

3. Roles and Responsibilities

3.1 Clients as Data Controllers; Moove and Geotab as Data Processors

The delivery of telematics services will require Moove and Geotab to process certain personal data as (independent) Data Processors on behalf of and in accordance with the instructions of Moove's clients as Data Controllers. As Data Controllers, clients are responsible for compliance with data protection law, in particular the legal basis for processing (e.g. consent, legitimate purpose, works council agreement, etc.), data subject rights and information obligations.

Moove will conclude the relevant Data Processing Agreements (DPA) according to Art. 28 GDPR with its clients.

Therefore, Moove

- processes personal data only on documented instructions from the client;
- will immediately inform the client if, in its opinion, an instruction infringes the GDPR or national data protection laws in the EU;
- ensures that persons authorised to process personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
- takes all measures required pursuant to Art. 32 GDPR (see point E below);
- assists the client by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the client's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III of the GDPR;

- assists the client in ensuring compliance with the obligations pursuant to Articles 32 to 36 GDPR (relating to security of personal data) taking into account the nature of processing of data and the information available;

- at the choice of the client, deletes or returns all of personal data to the client after the end of the provision of services relating to processing, and deletes existing copies unless EU or Member State law requires storage of the personal data;

- and makes available to the client all information necessary to demonstrate compliance with the obligations laid down in Art. 28 GDPR and allow for and contribute to audits, including inspections, conducted by the client or another auditor mandated by the client.

3.2 Compleye as a partner for achieving and maintaining the highest IT security standards

Moove appointed Compleye Coöperatie U.A. ("Compleye"), a company based in Amsterdam, the Netherlands, specialized in providing security and privacy advisory services via the use of comprehensive compliance management platform that facilitates the compliance with ISO27001 and 27701 standards and norms, as well as with applicable laws and regulations. For further information, see compleye.io.

Moove also contracts with other service providers in the area of IT security in order to be able to guarantee the highest level of IT security and resilience.

4. Privacy by Design: The "personal mode"

Clients can manually enable and disable the "personal mode" from the Geotab Drive app and the MyGeotab portal. The "personal mode" allows drivers and dispatchers to hide vehicle tracking in the fleet management application for designated periods of time. When "personal mode" is enabled, location features that use GPS such as: position, trips and speed profiles are not displayed in the application.

5. Data processing in the EU/EEA/third country data transfers

As a rule, the data processing by Moove takes place exclusively within the EU/EEA (no third country data transfer to avoid the „Schrems II" issue), so that the legal highest level of data privacy is ensured due to the applicable GDPR.

If and to the extent that Moove and/or Geotab transfer personal data to a country outside the EU/the EEEA ("third country") or process it there, this shall take place exclusively in the context of the provision of services and in compliance with the legally required guarantees to ensure an adequate level of data protection pursuant to Art. 44et. seq. GDPR, such as by concluding the current EU standard data protection clauses.

E. IT Security

Moove holds the ISO/IEC 27001:2013 ('ISO 27001') certification awarded by TÜV Nord, Netherlands. Moove is subject to annual audits performed by the external auditing firm required to maintain the ISO 27001 certification. The audit involves an independent and objective review of the Information Security Management System (ISMS) to ensure that the established policies, procedures, processes, and other controls are practical and efficient to meet the ISO/IEC 27001 standards requirement. Moove also implemented the Privacy Information Management System and obtained the ISO/iEC 27701 certification.

This said Moove makes every effort to adopt and implement such technical and organisational measures as may reasonably be expected to protect the personal data, in line with the purpose of processing, against accidental or unlawful destruction, accidental loss, unintentional modification and/or unauthorised disclosure or making available and all other forms of unlawful processing.

The security measures that are put in place are adapted to the level of data sensitivity by taking such measures that may reasonably be expected of Moove on the basis of the state of technology.

Sharing the same lean and agile approach, Moove has partnered with Compleye to find the perfect solution to the current compliance challenges with the aim to ensure the security and privacy of the data (Art. 32 GDPR) while keeping focus on the business growth and continuity and improving the efficiency and effectiveness in compliance. Guided by Compleye, Moove has implemented a series of security and privacy controls to face some of the biggest data security threats.

The overview of the technical and organizational data security measures available in Compleye Online that support our commitment to data security includes but is not limited to:

- The implementation of controls and policies that ensure data confidentiality, availability and integrity as well as employee awareness towards the potential threats and how to overcome them.
- The mitigation of risks and error and the definition of authorities and responsibilities are achieved through the segregation of duties.
- Access rights for users and accounts are restricted only to those who are absolutely required to perform routine, legitimate activities.
- Outstanding availability, uptime infrastructure monitoring, live migration, and top network throughout are secured as a result of choosing AWS Cloud Hosting and Google Cloud Platform.
- Personal data is retained for as long as required to provide the agreed services or otherwise required by the applicable laws and regulations, or until vehicle users exercise their right to have their data erased.
- To maintain live servers, secure and guarded against the external security threats, Moove uses the Malware detection tool that aims to identify resources that have already been compromised by malware, or those resources that are at risk. This includes the sources of such potential compromise.
- Reduced risk of data exposure achieved through limited access following the need-to-know and need-to-do principles.
- Moove implemented adequate cryptographic measures to prevent any data from being read, copied, modified or deleted by unauthorized parties, as outlined below:
    - Data encryption on production servers: The data on NVMe instance store volumes is encrypted using an XTS-AES-256 cipher, implemented on a hardware module on the instance.
    - Data encryption on databases: Amazon RDS encrypted DB instances use the industry-standard AES-256 encryption algorithm.
    - Moove owned devices used by its employees to store and process business and client data, have encryption enabled at all times.
    - All the data is served from the backend via HTTP REST APIs over TLS protocol. The connection is secured with SSL encryption using signature algorithm as SHA-256 with RSA Encryption. The certificate to sign the HTTPS calls is provided by AB-IT and is installed yearly.
- Key encryption managed using a key management system and regularly rotation of the certificates that can be automatically renewed.

- Penetration testing performed on its systems, through a trusted and independent security partner, to ensure that the systems remain secure and reliable.
- Moove conducts regular monitoring against external vulnerabilities to ensure that no potential security or privacy risks are created. Any vulnerabilities identified during the process are remediated in a timely manner.
- A sound Backup Policy and well governed processes which reaffirm Moove's commitment to providing the quickest transition and greatest quality of services possible through the backup arrangement, securing its client, business activities, and services from being jeopardized in any manner. Backup limitations are limited to the retention period of 4 weeks.
- Moove is subject to regular internal and independently conducted audits on its compliance with security policies and procedures, as well as on the adherence to the established security and privacy controls.

Moove established the stringent Recovery Point Objective (RPO) and Recovery Time Objective (RTO) values that serve as the key parameters of a disaster recovery and data protection strategy. The RPO and RTO are diligently monitored, evaluated and tested on a regular basis

Information about ensuring the highest level of IT security at Geotab is provided by the Geotab whitepaper „Best practices for cybersecurity management in telematics", publishes December 4, 2017 (available under https://www.geotab.com/white-paper/cybersecurity-management-telematics/) and in the Geotab **„Security Center"** (availabe under https://www.geotab.com/security/).

F. Conclusion

Moove goes the extra mile to protect privacy of its clients and their employees. This is backed up by the highest possible certifications and collaboration with amazing specialist in the field of data protection and IT security. If you have any remaining questions after reading this paper, please do not hesitate to contact us. We are happy to answer all your questions.

Get in touch

mooveconnectedmobility.com
info@mooveconnected.com