Graf von Westphalen

23 November 2022

Moove Connected Mobility B.V

Einhaltung der Datenschutz- und IT-Sicherheitsstandards

Dr. Michael Herold, M.C.L. Rechtsanwalt, Datenschutzbeauftragter (TÜV), Assoziierter Partner

moove®
people. fleet. impact.

Whitepaper

A. Zweck dieses Dokuments

Die Einhaltung der höchsten Datenschutz- und IT-Sicherheitsstandards ist für Moove Connected Mobility B.V. (im Folgenden „Moove“), für Ihr Unternehmen und Ihre Mitarbeitenden sowie für alle anderen Personen von zentraler Bedeutung.

Wir wissen und verstehen, dass Telematikdienste bei manchen Menschen Zweifel in Bezug auf den Datenschutz wecken. In diesem Whitepaper erklären wir Ihnen, wie Moove die höchsten Datenschutz- und IT-Sicherheitsstandards einhält, um die Privatsphäre jedes Einzelnen, mit dem wir arbeiten, zu schützen.

Moove hält sich nicht nur an die geltenden Datenschutz- und IT-Sicherheitsstandards und -vorschriften, sondern überwacht, aktualisiert und verbessert den Datenschutz und die IT-Sicherheit ständig – insbesondere im Hinblick auf Änderungen der Rechtslage, auch über das gesetzlich vorgeschriebene Maß hinaus.

B. In Zusammenarbeit mit GvW Graf von Westphalen

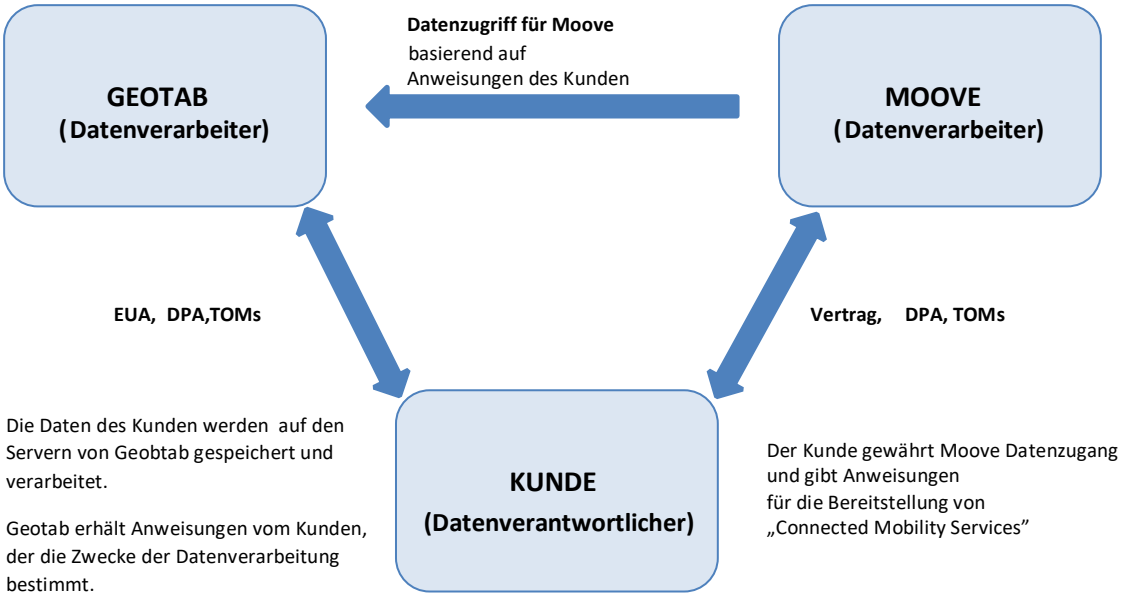
Dieses Whitepaper wurde in Zusammenarbeit mit GvW Graf von Westphalen (im Folgenden „GvW“) erstellt. GvW ist eine Sozietät mit mehr als 200 Rechtsanwältinnen und Rechtsanwälten sowie Steuerberaterinnen und Steuerberatern. Sie ist eine der größten unabhängigen Wirtschaftskanzleien in Deutschland. Eines der Fachgebiete von GvW ist die Digitalisierung und Technologie, einschließlich Datenschutz und IT-Sicherheit. Insbesondere die Mobilität und die digitale Vernetzung wirken sich zunehmend auf den Geschäfts- und Arbeitsalltag aus. Mit langjähriger, branchenübergreifender Erfahrung und fundiertem Fachwissen in allen wichtigen Rechtsgebieten bietet GvW Beratung in diesem Bereich an. Dabei stehen das Verstehen, Anwenden und Gestalten des rechtlichen Umfelds im Mittelpunkt.
GvW hat sich eingehend mit allen Prozessen von Moove befasst und billigt dieses Whitepaper.

C. Das Geschäftsmodell von Moove in Kürze – Flottentelematik

In Zusammenarbeit mit Geotab Inc. (im Folgenden „Geotab“), einem Unternehmen mit Hauptsitz in Oakville, Ontario, Kanada, und Tochtergesellschaften und Niederlassungen

weltweit, auch in Deutschland (Geotab GmbH, 52134 Herzogenrath, weitere Informationen unter geotab.com), bietet Moove Zugang zu einer breiten Palette von Telematikdaten. Diese Daten stammen aus dem Motormanagement (On-Board-Diagnose) und von zusätzlichen Geräten und Sensoren (Internet der Dinge). Auf der Grundlage dieser M2M-Daten, die Moove seinen Kunden über maßgeschneiderte Schnittstellen und Dashboards, die sogenannten „Connected Mobility Services“, zur Verfügung stellt, ermöglicht Moove seinen Kunden, ihre Geschäftsabläufe anzupassen und so die Verkehrssicherheit zu verbessern, die Fahrzeugwartung effizienter durchzuführen und/oder die Umweltbelastung zu verringern.

Beziehungen bei der Datenverarbeitung



D. Datenschutz

1. Grundlagen

Umfassende Informationen zum Datenschutz bei Moove finden Sie in der Datenschutzerklärung unter https://mooveconnectedmobility.com/app/uploads/2023/02/2115_Moove-Privacy-policy_DE.pdf.

2. Organisation

2.1 Mitarbeitende

Moove gewährleistet die Einhaltung des höchstmöglichen Datenschutzes und der höchstmöglichen Datensicherheit durch die Bereitstellung umfassender Informationen und regelmäßiger Schulungen sowie durch die strikte Verpflichtung der Mitarbeitenden zur Wahrung des Datengeheimnisses und der Vertraulichkeit.

2.2 Datenschutzbeauftragte

Moove hat eine (externe) Datenschutzbeauftragte ernannt, um sicherzustellen, dass die Rechte der betroffenen Personen gemäß den geltenden Datenschutzgesetzen und -verordnungen (BDSG und DSGVO) geschützt werden.

Die Datenschutzbeauftragte kann direkt unter angelika@compleye.io kontaktiert werden.

3. Aufgaben und Zuständigkeiten

3.1 Kunden als Datenverantwortliche; Moove und Geotab als Datenverarbeiter

Die Bereitstellung von Telematikdiensten macht es erforderlich, dass Moove und Geotab bestimmte personenbezogene Daten als (unabhängige) Datenverarbeiter im Auftrag und gemäß den Anweisungen der Kunden von Moove als Datenverantwortliche verarbeiten. Als Datenverantwortliche sind die Kunden für die Einhaltung der Datenschutzgesetze, insbesondere der Rechtsgrundlage der Verarbeitung (z. B. Einwilligung, rechtmäßiger Zweck, Betriebsratsvereinbarung usw.), der Rechte der betroffenen Personen und der Informationspflichten, verantwortlich.

Moove schließt die entsprechenden Auftragsverarbeitungsverträge (Data Processing Agreements – DPA) gemäß Art. 28 DSGVO mit seinen Kunden ab.

Moove

- verarbeitet personenbezogene Daten nur auf dokumentierte Anweisung des Kunden;

- informiert den Kunden unverzüglich, wenn seiner Meinung nach eine Anweisung gegen die DSGVO oder nationale Datenschutzgesetze in der EU verstößt;

- stellt sicher, dass die zur Verarbeitung personenbezogener Daten befugten Personen sich zur Vertraulichkeit verpflichtet haben oder einer entsprechenden rechtlichen Verschwiegenheitspflicht unterliegen;

- ergreift alle erforderlichen Maßnahmen gemäß Art. 32 DSGVO (siehe unten, Abschnitt E);

- unterstützt den Kunden durch geeignete technische und organisatorische Maßnahmen, soweit dies möglich ist, bei der Erfüllung der Verpflichtung des Kunden, auf Anfragen zur Ausübung der in Kapitel 3 der DSGVO festgelegten Rechte der betroffenen Person zu reagieren;

- unterstützt den Kunden bei der Einhaltung der Verpflichtungen gemäß Artikel 32 bis 36 DSGVO (in Bezug auf die Sicherheit personenbezogener Daten) unter Berücksichtigung der Art der Datenverarbeitung und der verfügbaren Informationen;

- löscht auf Wunsch des Kunden alle personenbezogenen Daten nach Beendigung der Erbringung von Dienstleistungen im Zusammenhang mit der Verarbeitung oder gibt diese an den Kunden zurück und löscht vorhandene Kopien, es sei denn, das Recht der EU oder eines Mitgliedstaats schreibt die Aufbewahrung der personenbezogenen Daten vor; und

- stellt dem Kunden alle Informationen zur Verfügung, die nötig sind, um die Einhaltung der in Art. 28 DSGVO festgelegten Verpflichtungen nachzuweisen, und lässt Prüfungen, einschließlich Inspektionen, durch den Kunden oder einen anderen vom Kunden beauftragten Prüfer zu und trägt zu diesen bei.

3.2 Compleye als Partner für die Erreichung und Aufrechterhaltung der höchsten IT-Sicherheitsstandards

Moove beauftragte Compleye Coöperatie U.A. (nachfolgend „Compleye“), ein Unternehmen mit Sitz in Amsterdam, Niederlande, das sich auf die Bereitstellung von Sicherheits- und Datenschutzberatungsdiensten durch den Einsatz einer umfassenden Compliance-Management-Plattform spezialisiert hat, die die

Einhaltung der Standards und Normen ISO 27001 und 27701 sowie der geltenden Gesetze und Vorschriften erleichtert. Weitere Informationen finden Sie unter compleye.io.

Moove schließt auch Verträge mit anderen Dienstleistern im Bereich der IT-Sicherheit ab, um ein Höchstmaß an IT-Sicherheit und Ausfallsicherheit gewährleisten zu können.

4. Datenschutz durch Design: Der „Privatmodus“

Kunden können den „Privatmodus“ manuell über die App Geotab Drive und das Portal MyGeotab aktivieren und deaktivieren. Der „Privatmodus“ ermöglicht es Fahrern und Disponenten, die Fahrzeugverfolgung in der Flottenmanagement-Anwendung für bestimmte Zeiträume auszublenden. Wenn der „Privatmodus“ aktiviert ist, werden Standortfunktionen, die GPS verwenden, wie z. B. Position, Fahrten und Geschwindigkeitsprofile, in der Anwendung nicht angezeigt.

5. Datenverarbeitung in der EU/EWR/Datenübermittlung in Drittländer

Die Datenverarbeitung durch Moove findet in der Regel ausschließlich innerhalb der EU/EWR statt (keine Datenübermittlung in Drittländer zur Vermeidung der „Schrems-II“-Problematik), sodass das rechtlich höchste Niveau des Datenschutzes aufgrund der geltenden DSGVO gewährleistet ist.

Falls und soweit Moove und/oder Geotab personenbezogene Daten in ein Land außerhalb der EU/des EWR („Drittland“) übermittelt bzw. übermitteln oder dort verarbeitet bzw. verarbeiten, geschieht dies ausschließlich im Rahmen der Erbringung von Dienstleistungen und unter Einhaltung der gesetzlich vorgeschriebenen Garantien zur Gewährleistung eines angemessenen Datenschutzniveaus gemäß Art. 44 ff. der DSGVO, etwa durch Vereinbarung der aktuellen EU-Standarddatenschutzklauseln.

E. IT-Sicherheit

Moove verfügt über die Zertifizierung nach ISO/IEC 27001:2013 („ISO 27001“), die vom TÜV Nord, Niederlande, vergeben wird. Zur Aufrechterhaltung der ISO-27001-Zertifizierung unterliegt Moove jährlichen Audits, die von der externen Wirtschaftsprüfungsgesellschaft durchgeführt werden. Das Audit beinhaltet eine unabhängige und objektive Überprüfung des Informationssicherheits-Managementsystems (Information Security Management System – ISMS), um sicherzustellen, dass die festgelegten Richtlinien, Verfahren, Prozesse und

anderen Kontrollen zweckmäßig und wirksam sind, um die Anforderungen der Norm ISO/IEC 27001 zu erfüllen. Darüber hinaus hat Moove das Datenschutz-Informationsmanagementsystem (Privacy Information Management System) eingeführt und die Zertifizierung nach ISO/IEC 27701 erhalten.

Dies bedeutet, dass Moove alle Anstrengungen unternimmt, um die technischen und organisatorischen Maßnahmen zu ergreifen und umzusetzen, die vernünftigerweise erwartet werden können, um die personenbezogenen Daten im Einklang mit dem Zweck der Verarbeitung vor versehentlicher oder unrechtmäßiger Zerstörung, versehentlichem Verlust, unbeabsichtigter Änderung und/oder unbefugter Weitergabe oder Bereitstellung und allen anderen Formen der unrechtmäßigen Verarbeitung zu schützen.

Die getroffenen Sicherheitsmaßnahmen werden dem Grad der Datensensibilität angepasst, indem solche Maßnahmen ergriffen werden, die nach dem Stand der Technik vernünftigerweise von Moove erwartet werden können.

In Zusammenarbeit mit Compleye, die den gleichen schlanken und agilen Ansatz verfolgen, sucht Moove nach der perfekten Lösung für die aktuellen Compliance-Herausforderungen. Ziel ist es, die Sicherheit und den Schutz der Daten (Art. 32 DSGVO) zu gewährleisten und sich gleichzeitig auf das Wachstum und die Kontinuität des Unternehmens zu konzentrieren sowie die Effizienz und Effektivität der Compliance zu verbessern. Unter der Anleitung von Compleye hat Moove eine Reihe von Sicherheits- und Datenschutzkontrollen eingeführt, um einigen der größten Bedrohungen der Datensicherheit zu begegnen.

Der Überblick über die technischen und organisatorischen Datensicherheitsmaßnahmen, die in Compleye Online zur Verfügung stehen und unser Engagement für die Datensicherheit unterstützen, umfasst unter anderem folgende Maßnahmen:

- die Implementierung von Kontrollen und Richtlinien, die die Vertraulichkeit, Verfügbarkeit und Integrität von Daten sicherstellen sowie die Sensibilisierung der Mitarbeitenden für potenzielle Bedrohungen und deren Bewältigung;
- die Minderung von Risiken und Fehlern sowie die Definition von Befugnissen und Verantwortlichkeiten werden durch die Trennung von Aufgaben erreicht;
- die Beschränkung von Zugriffsrechten für Benutzer und Konten auf diejenigen, die unbedingt erforderlich sind, um routinemäßige, legitime Aktivitäten durchzuführen;
- Sicherstellung von hervorragender Verfügbarkeit, Überwachung der Infrastruktur während der Betriebszeit, Live-Migration und ein durchgängig erstklassiges Netzwerk durch die Wahl von AWS Cloud Hosting und Google Cloud Platform;

- Aufbewahrung personenbezogener Daten über einen Zeitraum, der für die Erbringung der vereinbarten Dienstleistungen erforderlich ist, den die geltenden Gesetze und Vorschriften vorschreiben oder bis die Fahrzeugnutzer ihr Recht auf Löschung ihrer Daten ausüben;
- Gewährleistung der Sicherheit der Live-Server und deren Schutz vor externen Sicherheitsbedrohungen durch die Verwendung eines Tools zur Erkennung von Malware, das Ressourcen identifiziert, die bereits durch Malware kompromittiert wurden oder die gefährdet sind. Dazu gehören auch die Quellen einer solchen potenziellen Gefährdung;
- geringeres Risiko der Datenexposition durch eingeschränkten Zugriff nach dem Need-to-know- und Need-to-do-Prinzip;
- Ergreifung von angemessenen kryptografischen Maßnahmen, wie im Folgenden beschrieben, um zu verhindern, dass Daten von Unbefugten gelesen, kopiert, verändert oder gelöscht werden können:
    - Datenverschlüsselung auf Produktionsservern: Die Daten auf NVMe-Instance-Speichermedien werden mit einer XTS-AES-256-Verschlüsselung verschlüsselt, die in einem Hardwaremodul auf der Instanz implementiert ist;
    - Datenverschlüsselung in Datenbanken: Amazon RDS verschlüsselte DB-Instanzen verwenden den branchenüblichen AES-256-Verschlüsselungsalgorithmus;
    - Moove-eigene Geräte, die von seinen Mitarbeitenden zur Speicherung und Verarbeitung von Geschäfts- und Kundendaten verwendet werden, sind jederzeit verschlüsselt;
    - alle Daten werden vom Backend über HTTP-REST-APIs über das TLS-Protokoll bereitgestellt. Die Verbindung ist mit SSL-Verschlüsselung unter Verwendung des Signaturalgorithmus SHA-256 mit RSA-Verschlüsselung gesichert. Das Zertifikat zum Signieren der HTTPS-Aufrufe wird von AB-IT zur Verfügung gestellt und jährlich installiert;
- Schlüsselverschlüsselung mithilfe eines Schlüsselmanagementsystems und regelmäßiger Rotation der Zertifikate, die automatisch erneuert werden können;
- Penetrationstests der Systeme durch einen vertrauenswürdigen und unabhängigen Sicherheitspartner, um sicherzustellen, dass die Systeme sicher und zuverlässig bleiben;
- Durchführung einer regelmäßigen Überwachung gegen externe Schwachstellen, um sicherzustellen, dass keine potenziellen Sicherheits- oder Datenschutzrisiken entstehen. Alle während des Prozesses identifizierten Schwachstellen werden zeitnah behoben;

- eine solide Back-up-Politik und gut geregelte Prozesse, die das Engagement von Moove bekräftigen, den schnellstmöglichen Übergang und die bestmögliche Qualität der Dienste durch die Back-up-Vereinbarung zu gewährleisten, und die Kunden, Geschäftsaktivitäten und Dienste vor jeglicher Gefährdung schützen. Die Datensicherung ist auf eine Aufbewahrungsfrist von vier Wochen beschränkt;
- regelmäßige Durchführung interner und unabhängig durchgeführter Audits zur Einhaltung der Sicherheitsrichtlinien und -verfahren sowie zur Befolgung der festgelegten Sicherheits- und Datenschutzkontrollen.

Moove hat die strengen Werte für das Recovery Point Objective (RPO) und das Recovery Time Objective (RTO) festgelegt, die als Schlüsselparameter eines Disaster-Recovery-Plans und einer Datensicherungsstrategie dienen. Das RPO und RTO werden regelmäßig sorgfältig überwacht, bewertet und getestet.

Informationen über die Gewährleistung des höchsten Niveaus an IT-Sicherheit bei Geotab finden Sie im Whitepaper „Best Practices für Stärkung der Cyber-Sicherheit in der Telematik“, das Geotab am 4. Dezember 2017 veröffentlicht hat (verfügbar unter https://www.geotab.com/de/white-paper/cybersicherheit-telematik/) und im **Geotab-Sicherheitszentrum** (https://www.geotab.com/de/sicherheit/).

F. Fazit

Moove geht die Extrameile, um die Privatsphäre seiner Kunden sowie deren Mitarbeitenden zu schützen. Dies wird durch die höchstmöglichen Zertifizierungen und die Zusammenarbeit mit hervorragenden Spezialistinnen und Spezialisten auf dem Gebiet des Datenschutzes und der IT-Sicherheit untermauert. Sollten Sie nach der Lektüre dieses Whitepapers noch Fragen haben, kontaktieren Sie uns gerne. Wir freuen uns, alle Ihre Fragen beantworten zu dürfen.

Sprechen Sie uns an

mooveconnectedmobility.com
info@mooveconnected.com