VIANOVA'S GDPR STATEMENT

July 2021

Table of contents

Introduction

Mobility data is a crucial resource for thoughtful decision and policy-making in urban environments, whether by municipalities, transport authorities, mobility operators or businesses. If understood and used correctly, it may help create smarter, more secure and more inclusive cities, for the benefit of all citizens and customers.

The use of mobility data also raises various legitimate privacy concerns, especially about the potential outcomes of ill-intentioned surveillance of travellers.

At Vianova, we believe that such concerns must not be dismissed, but also that they can be addressed adequately while still making the most out of the vast potential of mobility data.

This document is our GDPR statement. It reflects the way we comply with the world's most stringent privacy regulation, the EU General Data Protection Regulation.

It will answer most questions about what we do at Vianova and how we do it. If it does not, please feel free to contact us using our email addresses below!

What types of data does Vianova collect?

► We collect and process mobility data, i.e. data relating to vehicles - whether shared, personal or professional. We do not, however, collect any data that directly identifies individuals such as user profiles or credit card identification.

Our services are based on both quantitative and qualitative analyses of mobility data. Depending on the project, we ingest data relating to shared vehicles (e.g. free floating e-scooters or dockless bikes), professional vehicles (e.g. taxis or delivery services) and personal vehicles (e.g. personal connected cars).

Vianova does not presently generate any mobility data itself, but rather relies on partners who generate this data. Data is collected from operators and manufacturers themselves, and comes in a variety of standard formats, such as Mobility Data Specification (MDS), General Bikeshare Feed Specification (GBFS) and City Data Standard Mobility (CDS-M) for shared mobility data and Floating Car Data (FCD) for connected cars. Some data collected does not presently adhere to an international technical standard because the data provider may use their own proprietary standard.

In general, datasets include a combination of vehicle unique identifiers (vehicle IDs), quasi real-time and/or historical geolocation data and information relating to the current and/or past condition of the vehicle (e.g. functioning/non-functioning, low battery, etc). When we collect quasi real-time data, we make sure that a sufficient delay elapses after the end of the considered trip before collecting the data, to avoid real-time surveillance risks.

These data are used in the context of our services to provide smart analytics and to allow the monitoring of professional fleets, on-demand mobility, shared vehicles or last-mile delivery services.

However, **we *do not* collect any directly identifying information** such as names or email addresses of end users, drivers or vehicle owners.

In Depth: What is MDS?

MDS is an open-source, collaborative, mobility data format governed by a non-profit organisation (the Open Mobility Foundation (OMF)). It is widely used in the USA and is getting strong traction across Europe.

MDS datasets include unique vehicle identifiers (vehicle IDs), combined with real-time and historical location data. They allow municipalities to better understand mobility patterns on their territory, but also to tackle most challenging issues raised by the multiplication of shared micro-mobility vehicles.

Using MDS data is especially relevant in enabling municipalities to craft and enforce slow-speed areas, restricted parking areas and other local traffic policies. It will also help authorities locate and remove abandoned, dysfunctional or out-of-battery vehicles. Municipalities may also use MDS-derived mobility insights for other purposes such as urban planning with the development of cycling lanes, mobility orchestration for large events, etc.

Although the first use cases for MDS were managing and analyzing micro-mobility services, the use of MDS and other standards governed by OMF are now expanding to other services such as car-sharing services, and maybe soon ride-hailing services and urban logistics.

Vianova is a member of the Open Mobility Foundation and is proud to lead the adoption of g MDS inEurope, in compliance with local laws and regulations.

How is such mobility data subject to GDPR?

► The answer depends on the types of vehicles generating data. In general, geolocation data and vehicle IDs (and any data associated with such vehicle IDs) will qualify as personal data, and as such be subject to GDPR.

GDPR is about the protection of *personal data*, i.e. data which relates to an identified or identifiable person (Article 4.1 GDPR); a person is said to be identifiable when another person (e.g. Vianova or a person using our services) may re-identify them through means which are reasonably likely to be used (Recital 26 GDPR).

This concept of personal data has been interpreted very broadly by European courts and supervisory authorities, with much literature about its application to mobility and geolocation data (see below) - although none of it specifically about shared vehicles.

Among the different types of data we collect and process, the following must qualify as personal data, and - as such - is subject to GDPR:

- ❏ "Native" vehicle IDs of shared and professional vehicles (i.e. unique vehicle identifiers attributed by the operator or manufacturer);
- ❏ Any data which may be associated with such a native vehicle ID (e.g. geolocation data, vehicle condition or other vehicle IDs which may be retraced to the native ID); and
- ❏ Non-aggregated geolocation data of shared, personal and professional vehicles.

All of these data are only ***indirectly identifying*** **(or "pseudonymized") personal data**, i.e. data which allows for the re-identification of a given individual only when combined with other, directly identifying personal data. Such indirectly identifying/pseudonymized personal data is generally considered by the supervisory authorities to be much less sensitive than directly identifying personal data.

Also, many data we collect or process will qualify as **anonymized data**, either because it did not allow for re-identification of a given individual even at the time we collected it, or because we have processed it in such a way that makes such re-identification highly unlikely. Irreversibly aggregated information about trips or vehicle distribution, for instance, will qualify as anonymized data, and as such is not subject to GDPR.

We may process both pseudonymized and anonymized data depending on what is necessary to fulfil the use case at hand (data minimization). Where it is sufficient, we will only collect and process anonymized data; on the other hand, certain use cases such as enforcement of regulations imposed on mobility operators and audit of data quality will require single data points. This distinction is why it is so critical that cities and other users of mobility data be explicit in the use cases they are looking to fulfill, because it guides the data necessary to accomplish the task.

Is it lawful to collect and process such personal data?

► Yes. GDPR is not about prohibiting the collection or processing of personal data or making it unlawful. It is about setting up appropriate safeguards for individuals' privacy.

It is - unfortunately - a very common misconception that GDPR prohibits the collection and processing of personal data. A related misconception is that GDPR would only allow for the processing of anonymized data, i.e. non-personal data.

Both these misconceptions are debunked within the very title of GDPR, which is explicitly about the ***protection*** **of personal data** within an environment which the free flow of data is to be encouraged. Such free flow is also advancedby other EU directives and regulations such as the 2019 open data directive.

GDPR is only about making sure that appropriate guarantees and safeguards are set up when processing personal data; such guarantees and safeguards may especially include the

pseudonymization of data, which differs from anonymization in that pseudonymization is reversible (i.e. data may still be retraced to a given individual). Other techniques include data minimisation as previously mentioned, access controls, and retention policies as will be further discussed.

Is such mobility data sensitive data within the meaning of GDPR?

► Strictly speaking, no. Plus, we process mobility data in such a way that prevents it from revealing sensitive information about individuals' daily lives.

Sensitive data under GDPR (Article 9.1 GDPR) means data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, health data, sex life or sexual orientation. Neither mobility data nor geolocation data falls within this definition *per se*.

However, supervisory authorities' guidelines and opinions underline that geolocation data should be considered sensitive inasmuch as it may reveal intimate details about the daily lives of drivers/vehicle owners. This is based on the assumption that mobility patterns of a personal vehicle are recurring and consistent enough to draw conclusions on - for instance - home or workplace locations.

We collect, aggregate, **pseudonymize and anonymize mobility data** in such a way that does not allow for such intimate details to be revealed, especially by making a clear distinction between data relating to shared vehicles, professional vehicles and personal vehicles.

Is data subjects' consent necessary to collect such mobility data ?

► In this case, no. GDPR allows for many cases where personal data may be processed without data subjects' consent; it all depends on how and why.

Consent is not the only or primary legal basis for processing personal data under GDPR (Article 6.1 GDPR). Consent is even non applicable in certain cases, e.g. where there is an imbalance of power or authority between the data controller and individuals whose data is collected, so that consent in such cases is not considered freely given.

Another legal basis to process personal data is the pursuit of a **legitimate interest**, provided that such legitimate interest is not overridden by the interests or fundamental rights and freedoms of the data subjects (Article 6.1.f) GDPR). This basis depends on a close assessment, to be conducted on a case-by-case basis.

After conducting this assessment in compliance with supervisory authorities' guidelines, we have come to the conclusion that our processing of mobility data is justified not only by Vianova's legitimate interest in providing our services, but also by citizens' legitimate interest in benefitting from a more secure, reliable and inclusive urban environment. This interest is long recognized and promoted by the EU regulations on transport and smart cities, such as the Directive on Intelligent

Transport Systems (ITS) and the 2019 Open Data Directive, which deems mobility data "high value data" and encourages its sharing within Member States.

Who gets to access the data? Who exactly is in charge of what?

► Simply put: the Vianova teams, our 3rd-party hosting service providers, and (to a limited extent only) our clients. GDPR obligations and responsibilities are clearly identified and allocated depending on the role and capacities of each party.

We collect mobility data through secured, state-of-the-art APIs and host it on servers provided and managed by a top-tier hosting service provider. We have access control in place to make sure it may only be consulted by the relevant team members within Vianova.

Although the aggregated and anonymized analytics provided by Vianova to our clients is typically sufficient to fulfill most needs, certain mobility data may be shared with clients for the purpose of our mobility management services; in any case, we take appropriate measures to minimize, pseudonymize and limit retention of such data, in compliance with GDPR principles. In other words, in order to fulfill a specific use case, a client may be able to obtain mobility data for individual trips or devices, but Vianova will work with the client to avoid re-identification of individuals through that data.

All our agreements - with mobility operators, our technical service providers and our clients - include appropriate clauses to clarify each party's responsibility and organize compliance with GDPR and data protection principles (Articles 26 and 28 GDPR), with standard contractual clauses from the European Commission in case data is transferred to a country out of the EU (Article 46.2 GDPR).

Our role and qualification in this context is generally that of a **data controller**, meaning we take responsibility for the compliance of our processing of mobility data with all applicable GDPR provisions, including those of data minimization, limitation of storage, legal basis and relationships with data subjects.

Alternatively, in certain specific cases, depending on instructions we receive from our clients, we may qualify as **data processor**. In such cases, the client is the data controller. As data processors, we offer the most robust guarantees in terms of data security, confidentiality and assistance, as materialized in our data processing agreement (available by request).

Focus: Being a data controller vs a data processor

The GDPR qualifications of data controller and data processor come with a different set of prerogatives.

The data controller (i.e. the person or entity who determines the purposes and means of processing the data) is especially responsible for the lawfulness of the processing and, as applicable, information and consent of data subjects; in contrast the data processor is responsible

for processing the data on the controller's instructions only and ensuring the security and confidentiality of data only processing it.

This distribution of prerogatives is to be materialized in a specific *data processing agreement*, the content of which is dictated by Article 28 of GDPR.

So, how exactly do you ensure GDPR compliance?

► We have performed in-depth, cutting-edge analyses of our technologies and business models; we make continuous efforts to stay at the top of GDPR best practices on the mobility data market.

We have performed a **comprehensive, in-depth data protection impact assessment (DPIA)** (Article 35 GDPR) to make sure that our practices comply with GDPR and respect individuals' privacy. To the best of our knowledge, this DPIA is the first initiative of its kind in the field of mobility data worldwide.

We have reduced our collection of data to that which is strictly necessary to provide our services (Article 5.1.c) GDPR) and we take steps to delete/anonymize within a brief delay, as soon as it is not necessary to retain raw data anymore for individual vehicle monitoring (generally within a few days or weeks) (Article 5.1.e) GDPR).

We use state-of-the-art security measures to protect mobility data while at rest, in motion and in use, by relying on top-tier global service providers and leading technologies(Article 32 GDPR). Data we collect and process is stored on servers located in the EU (Frankfurt). We have appointed a data protection officer (Article 37 GDPR) in the person of an external specialized lawyer.

We process and answer every data subject's request for exercise of a right under GDPR, i.e. requests relating to the right of access (Article 15 GDPR), right to rectification (Article 16 GDPR), right to erasure (Article 17 GDPR), right to restriction of processing (Article 18 GDPR) and right to object to the processing (Article 21 GDPR). We also comply with data subjects' right to lodge a complaint with the competent supervisory authority.

We will continue improving and updating these measures constantly, as necessary to follow data protection regulations and best practices.

What about the Law Enforcement Directive?

► It is about the processing of personal data by certain public authorities. As such, we are not subject to it; however, some of our clients may be.

The Law Enforcement Directive (i.e. Directive (EU) 2016/680) applies to "*the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security*".

As Vianova is not a "competent authority" within the meaning above, our own processing of mobility data is not subject to this Directive, but to the GDPR only.

However, if you are a competent authority within the meaning above and receive mobility data (other than anonymized data) from us, you must consider complying with the Law Enforcement Directive. The principles of this Directive are mostly the same as those of GDPR but, as a directive may be transposed differently into the different Member States' domestic laws, we recommend that you check it with your local legal advisor.

Are there any other data confidentiality concerns I should be aware of?

► Clients should be aware that insights provided by Vianova may include sensitive commercial information about the operations of mobility service providers.

Though this aspect is not subject to GDPR or privacy regulations, some of the insights derived from mobility data may include information that is sensitive to operators. For example, when metrics are sorted by operator, certain business information is visible such as the utilization of devices (and by extension their profitability). Vianova's clients should be careful to limit access to commercially sensitive data to those within the organization that have a need for it in order to fulfill their use cases (for example, for fining operators for non-compliance with policies and regulations).

Vianova encourages the presentation of some aggregated, anonymized insights to the general public, either through periodic reports or as an open data set on the city's open data tal. Such insights could include the total number of trips or devices, the most popular origins and destinations, or the most popular times of day. However, public agencies publishing this data should be careful to either aggregate that data across all providers, or to delay release of the data until it is no longer commercially valuable.

Why should I trust this GDPR statement?

► Don't just take our word for it: this is all based on a thorough analysis of supervisory authorities' guidelines and case law from the EU Court of Justice.

This GDPR statement reflects our own data protection impact assessment (DPIA), which we conducted with the help and support of a specialized law office.

Our DPIA was grounded on an exhaustive analysis of relevant supervisory authorities' guidelines and opinions and case law from the EU Court of Justice, including in particular:

- ❏ **The European Data Protection Board**'s guidelines on connected vehicles and on transparency;
- ❏ Former **Article 29 Working Party**'s opinions on Cooperative Intelligent Transport Systems, on geolocation services, on the concept of personal data, on anonymization techniques and on the notion of legitimate interest;

- ❏ The **French supervisory authority (CNIL)**'s compliance framework on connected vehicles and simplified standard on geolocation of professional vehicles.

This statement is also based on our rich experience of dealing with mobility data and related privacy concerns in close cooperation with municipalities, transport authorities and mobility operators.

Where can I get more information?

► ***Just get in touch with us. We are always happy to talk!***

Should you have any concern or question in relation to this GDPR Statement, please feel free to contact us (thibault.castagne@vianova.io, thibaud.febvre@vianova.io) and our data protection officer (dpo@vianova.io).

We will be happy to provide you with further information about the way we can make the most out of mobility data in a GDPR-compliant manner!

About this statement

This statement and its content are intended to explain how VIANOVA has designed its services to comply with GDPR, and how we help municipalities and transport operators handle mobility data in compliance with GDPR. It does not constitute legal advice, nor should it be a substitute for legal advice. Practitioners should always consider existing laws in their local jurisdiction.

Any content extracted from this document must be accompanied by a statement identifying Vianova as the publisher and the publication from which it originated as the source.

Citation: Vianova, Inc. (2021). GDPR Statement. Retrieved from: https://www.vianova.io/